Working with you to make Sheffield HEALTHIER

NHS Sheffield Clinical Commissioning Group

Confidentiality Code of Conduct and Data Protection Policy

November 2018

Version:	4.0
Date ratified:	20 November 2018
Policy Number	CO993/11/2020
Name of originator/author:	Head of Information, Performance and PMO
Name of Sponsor:	Director of Commissioning and Performance
Name of responsible committee	Governance Sub Committee
Date issued:	November 2018
Review date:	November 2020
Target audience:	All staff working within or on behalf of NHS Sheffield CCG

To ensure you have the most current version of this policy please access via the NHS Sheffield CCG Intranet Site by following the link below:

http://www.intranet.sheffieldccg.nhs.uk/policies-procedure-forms-templates.htm

disability confident EMPLOYER

Policy Audit Tool

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

Please give status of Policy:	**New / Revised**

1.	**Details of Policy/Procedural Document**	
1.1	Policy Number:	CO003/11/2020
1.2	Title of Policy/document:	Confidentiality Code of Conduct and Data Protection Policy
1.3	Sponsor	Information Governance Group
1.4	Author:	Sandie Buchan, Head of Information, Performance & PMO
1.5	Lead Committee	Governance Sub Committee
1.5	Reason for policy/document:	Sets out how the CCG works with confidential information
1.6	Who does the policy affect?	All staff working within or on behalf of NHS Sheffield CCG
1.7	Are the National Guidelines/Codes of Practice etc issued?	
1.8	Has an Equality Impact Assessment been carried out?	Yes
2.	**Information Collation**	
2.1	Where was Policy information obtained from?	Previous Policy & Information Governance expertise
3.	**Policy Management**	
3.1	Is there a requirement for a new or revised management structure for the implementation of the Policy?	No
3.2	If YES attach a copy to this form.	
3.3	If NO explain why.	
4.	**Consultation Process**	
4.1	Was there external/internal consultation?	Internal
4.2	List groups/persons involved	Information Governance Group, EMBED IG Team
4.3	Have external/internal comments been included?	Yes
4.4	If external/internal comments have not been included, state why.	
5.	**Implementation**	
5.1	How and to whom will the policy be distributed?	All CCG staff Internal Intranet
5.2	If there are implementation requirements such as training please detail.	
5.3	What is the cost of implementation and how will this be funded	

6.	Monitoring	
6.1	How will this be monitored	Number of adverse incidents reported Number of complaints received IG Training completed by all staff. Completion of Data Security & Protection Toolkit on an annual basis. Data Security & Protection Toolkit requirements are met.
6.2	Frequency of Monitoring	Monthly, Quarterly, Annually – dependent on the type of monitoring

Version Control

VERSION CONTROL				
Version	**Date**	**Author**	**Status**	**Comment**
2.0	**July 2014**	**Information Governance Group**		
3.0	**April 2016**	**EMBED IG Team**	**Review**	**Key IG Roles responsibilities added.** **References to CSU amended** **IAOs given responsibility for legality of information transfers.** **Section 14: Added reference to Health & Social Care (Safety and Quality) Act 2015.** **Section 20: added specific rank requirement for requests for personal information from the police.** **Allowed for lawful and reasonable non-consented disclosures of personal info** ***Note section 23 will be updated / added when the "Remote Working & Portable Devices Policy" has been finalised.***
4.0	**August 2018**	**EMBED IG Team**	**Review**	**Updates to align with GDPR/ DPA2018** **Minor changes for clarity** **IG Incident reporting requirements updated** **Listed EMBED for secure disposal of electronic devices** **Access to Records section updated** **Email encryption guidance added**

Contents

1 Introduction & Purpose

In the operation of the organisation, commissioning and the delivery of effective care, NHS Sheffield Clinical Commissioning Group (the CCG) obtains, holds, uses and discloses confidential information. This confidential information may be:

- Information about named individuals (including service users, carers, members of staff and other third parties)
- Information about the CCG, other health or social care organisations or contractors (such as records relating to finance, risk, tenders, contracts etc.[1])

Keeping information confidential is not the same as keeping it secret. It is essential that relevant, and proportionate, access to confidential information is available to those who have a need to know it in order to do their work. Balancing the need to keep information confidential with appropriate sharing may not always be straightforward and advice should be sought where there is any doubt.[2] Recent changes in legislation, the reconfiguration of the NHS and the diversity of service provision in the modern health care system involving close working relationships across different professional groups and health and non-health care agencies, may make it harder to understand what information it is permissible to share and in what circumstances.

This code of conduct is intended to enable the CCG and its staff (including non-CCG staff with access to CCG information) to work effectively in a confidential manner for the benefit of the population of Sheffield and other users of our services. It should help protect patients / service users and staff from the misuse of their information and ensure that confidential information is handled in a lawful and appropriate manner by:

- Defining what is meant by the phrase “confidential information”
- Informing staff of their responsibilities in relation to such information
- Informing staff of the correct procedures for dealing with confidential information so that they do not inadvertently breach confidentiality
- Providing sources of further information

Staff should ensure they are familiar with the content of this Code of Conduct. In particular, they should read section 5 – Good Practice, which outlines the principles and requirements of confidentiality that they are most likely to be relevant.

If you have any questions about the code you should contact your line manager in the first instance or the Information Governance Lead.

2 Scope

- This code of conduct applies to all NHS Sheffield CCG employees and non-CCG employees who work within the CCG or under contract to it. This includes, but is not limited to, staff on secondment to the CCG, students on placement, commissioning support services staff, and people working in a voluntary capacity.

- For convenience, the term ‘staff’ is used in this document to refer to all those to whom

[1] Not all of the information will be confidential. Some of the information we hold it may be disclosable under the Freedom of Information Act. Please contact the IG FOI Lead for advice.

[2] The CCG’s Caldicott Guardian, Senior Information Risk Owner and the EMBED IG team can provide advice.

the code of conduct applies.

- All staff are expected to comply with this code of conduct.

- The duty of confidentiality arises out of common law, legal obligations, staff employment contracts and professional obligations.[3]

- This duty continues after the staff member no longer works for/has an association with the CCG.

- Any breaches of this code including unauthorised breaches of confidentiality, inappropriate use of personal health or staff records or abuse of computer systems will be treated as a disciplinary offence, which may result in your employment, or association, with the CCG being terminated. It may also bring into question your professional registration[4] and possibly result in legal proceedings. This will also be the case for breaches of commercial confidentiality.

- If there is anything that is not clear or which you do not understand, you must contact your line manager, in the first instance, or the Information Governance Lead for further information.

3 Definitions

CCG:	Clinical Commissioning Group
PCD:	Personal Confidential Data
SIRO:	Senior Information Risk Owner
IAO:	Information Asset Owner
IG:	Information Governance
GDPR:	General Data Protection Regulation
DPA:	Data Protection Act
FOI:	Freedom of Information
EIR:	Environmental Information Regulations

4 Process/Requirements

- The CCG **Caldicott Guardian** is responsible for approving uses of personal confidential data (PCD). They are a Governing Body/Executive level lead who acts as the conscience of the organisation in relation to the use of patient data. Their role is to ensure the organisation processes personal confidential data lawfully and ethically.

- The CCG **Senior Information Risk Owner (SIRO)** is a Governing Body/Executive level person who has overall responsibility for ensuring the organisation handles all personal and organisational information appropriately and lawfully and that processes are in place to manage information risk.

- CCG information assets must be assigned an **Information Asset Owner (IAO)**. It is the responsibility of the IAO to ensure the assets under their control are protected from unauthorised access; that risk assessments are carried out at least annually and that all transfers of personal information from their assets are legal.

[3] For example, with the General Medical Council, Nursing and Midwifery Council or Health Professions Council

[4] See note 4 above

- **All managers** are responsible for ensuring that the staff they manage are aware of this Code of Conduct and their individual responsibility for complying with it. They should ensure their staff are equipped to fulfil those responsibilities; this will include by covering it at local induction and by identifying and meeting specific and generic training needs through personal development plans. Senior managers should ensure that managers within their Service area are aware of their responsibilities in relation to staff awareness.

- Managers should ensure ALL new staff have signed the Confidentiality and Information Security declaration. Managers are required to countersign this declaration to indicate that they have checked that the member of staff has read the relevant information governance policies and has had an opportunity to ask questions about anything they do not understand.

- **All staff** must ensure that they are aware of the requirements and standards of behaviour that apply and comply.

- **All staff** are responsible for reporting information incidents and near misses including breaches of confidentiality and information security in line with the CCG's Incident Reporting Policy.

- The CCG's incident reporting process can be obtained from line managers in the first instance and is also available on the CCG's intranet.

- The Information Governance Group is responsible for overseeing the implementation of this Code of Conduct including monitoring compliance. It is responsible for ensuring it is reviewed periodically.

- **Contact details** of key IG contacts (for example, the Caldicott Guardian and SIRO) will be made available on the CCG intranet.

5. Good Practice Guidance	**If the information you are looking for is not covered in this section you should contact your line manager or the Information Governance Lead for advice. Many of the information governance issues are interlinked so it is difficult to provide information about one topic in isolation.**
Confidentiality	1. What is **confidential information**? 2. Who has a **duty of confidentiality**? 3. Why is **confidentiality important**?
Staff Responsibilities	4. **Inform** patients/service users and staff about how we use their information 5. **Record** information **accurately**, **consistently** and in a **timely** manner 6. Dispose of **confidential waste** appropriately 7. **Be aware of and use confidential information** in accordance with CCG **policies** 8. **Apply** CCG **policy** within **your sphere of influence** 9. **Improve standards** of practice wherever possible 10. **Report incidents** and **near misses** in line with CCG policy 11. Use **social networking media** appropriately
Patient/Service User/Staff Rights	12. The **rights** of **individuals** in relation to **their information** (including the right to access personal information)
Consent	13. **Consent to obtain** information 14. **Consent to use and share** personal information 15. **Consent: capacity** to consent 16. **Consent: children** and **young people**
Disclosing Personal Information	17. Dealing with **requests for personal information** (including access to the health records of deceased people)

	18. **Reasons** for **disclosing** information **without consent** 19. **Procedure** for **disclosing** information **without consent** 20. **Procedure** for **disclosing** information to the **police** 21. **Check list** of points that must be considered **before disclosing** confidential information 22. **Safe havens** and safe haven **procedures**
Information Security	23. Use of **portable devices** (such as **USB sticks**) 24. **Information Secure storage**, use and transfer 25. **Working from home**
Using data for secondary uses	26. **Rules** regarding the **use of patient identifiable information** for non-direct care (secondary uses)
Freedom of Information Act, Environmental Information Regulations	27. **Freedom of Information Act, Environmental Information Regulations** and **requests** for information

Good Practice

Topic	What this means in practice
Confidentiality	
1. What is confidential information?	Confidential information may be information about identifiable individuals including, but not limited to, patients/service users, carers, member of staff or other third parties. It may also be organisational "corporate" information about the CCG, any other health or social care organisation, or external third party. It is not necessary for the name of the individual to be known for the information to be identifiable. For example, it may be possible to identify an individual when a number of data items are put together such as post code, ethnicity and medical condition or job role and ethnicity. Within the NHS, information about deceased people is not treated any differently to that of living people, that is, the duty of confidentiality extends beyond death. Confidential information may be in a variety of forms including but not limited to electronic, paper, digital or audio format, such as records, note books, message books, x-rays, photographs, audio tapes, voicemail etc., or it may be knowledge gained from overheard conversations or seeing someone sitting in a clinic waiting room. Examples of confidential information the CCG holds include: • Personal demographic details of staff (and patients/service users) • Contact details of staff (and patients or service users) • Medical details of staff (and patients or service users) • Ethnicity of staff (and patients or service users) • Bank and salary details of staff and financial details of service users • Results of Disclosure and Barring Service checks • Organisational financial information • Information that is defined as commercial in confidence under the Freedom of Information Act 2000 • Information in relation to concerns and complaints Information that has been placed in the public domain, except as a result of a breach of confidentiality, is not classed as confidential.

2. Who has a duty of confidentiality?	All CCG employees, and non-CCG employees who work with Sheffield CCG or under contract to it, have a duty to maintain the confidentiality of information gained during their employment/association with the CCG. This includes, but is not limited to, commissioning support services staff, staff on secondment to the CCG, students on placement and people who are working in a voluntary capacity. For convenience, the term 'staff' is used in this document to refer to all those to whom the code of conduct applies. Anyone may come into contact with confidential information in the course of their duties. For example: • You may have direct access to confidential information if you are authorised to access information held in: staff or patient/service user records; records about complaints, incidents, safeguarding; a register of concerns; contracts etc. • You may have confidential information passed to you in connection with your work • You may become aware of information as a result of breaches of confidentiality You are legally obliged to maintain the confidentiality of this information. This duty continues after you no longer work for/have an association with the CCG.
3. Why is confidentiality important?	Confidentiality is important to protect the privacy of all individuals, both staff and patients and the commercial confidences of third parties, whose information we hold, to enable the CCG and its partners to conduct their business effectively. Both staff and service users provide the CCG with confidential information about themselves in the course of the CCG's business activities. They have a legitimate expectation that we will respect their privacy and treat their information appropriately. As part of the wider NHS and in delivering its own services, it is important that the CCG maintains the trust of patients. Patients and service users entrust health services with, or allow us to gather, confidential information relating to their health and other matters when they access our services. We use this information to assess their needs and deliver appropriate treatment and care; including an audit of such care. We also use this information in a pseudonymised form for secondary purposes such as the planning and management of services. It is essential that clinicians and practitioners have all relevant information to hand when treating or caring for people. If patients and service users do not trust us with their information

	they may withhold vital information or not seek treatment. In addition, services may be planned on the basis of inaccurate information about the health needs of the population. In some circumstances, service users may lack the competence to extend their trust or may be unconscious, but this does not diminish the duty of confidence. Trust is important in managing health and safety, and risk. Staff or patients may want to pass on information about other individuals, for example, to report poor practice/incidents/near misses. Staff should be aware of the appropriate procedures, which should be followed in such cases. The CCG works in partnership with partner organisations and third parties in order to discharge its duties. Lack of confidence in the CCG's ability to maintain confidentiality would seriously impede the CCG from operating effectively. It is essential if the trust of staff and patients/service users is to be retained, and legal requirements are to be met, that the NHS provides, and is seen to provide, a confidential service.
Staff responsibilities	
4. Inform staff about how we use their information	Being open and transparent with people about who you are, what your role is, why you are collecting information, how we will use it, who we may share it with and gaining informed consent is not only integral to processing information fairly under the Data Protection Act 2018 / GDPR, but is at the heart of addressing many issues around information sharing and confidentiality. This guidance refers to both contact with patients and staff. Individuals who provide us with information should do so on the basis that they understand how that information might be used At a patient's, service user's or member of staff's **first contact** with the organisation or service, or at the most appropriate time thereafter, a member of staff should: • Explain to them why we collect information, how it might be used, who it might be shared with and seek their consent. • Make it clear to individuals what your role is and the circumstances under which confidential information may have to be shared. This gives them the opportunity to make an informed choice as to what information they disclose to us. • Explain to patients and service users that the information they give may be recorded, may need to be shared in order to provide them with optimal care and may be used to support clinical audit, service evaluation and other work to monitor the quality of care provided. • Explain to individuals their general rights (see section 12). • Consider if individuals would be surprised to learn that their information is being used in a particular way. If they would

	be surprised, they are not being effectively informed and this may lead to mistrust in the professional and the organisation. Unless there is a legal reason not to, patients and service users should normally be asked before their personal information is used in ways that do not directly contribute to, or support the delivery of, their care. Their decisions to restrict the disclosure of their personal information should be respected. Staff should consider the following options to ensure patients and service users are effectively informed: • Has the patient or service user been provided with a generic information leaflet or a service specific information leaflet? • Have they had the opportunity to read the leaflet and ask questions? • Is it clear to them when information is recorded or health records accessed? • Is it clear to them where staff are already, or will be, sharing information with others? • Are they aware of the choices available to them in respect of how their information may be used or shared? • Have you checked that the patient or service user has no concerns or queries about how their information is used or shared? • Do they have a learning disability, alternative communication needs, capacity issues that requires additional or specialist support in order to engage with them as fully as possible? • Answer any queries personally or direct the patient or service user to others who can answer their questions or to other sources of information. The EMBED Information Governance Team can also be contacted by staff for assistance. • Respect the rights of patients and service users and assist them in exercising their right to have access to information held in their health records.

5 Record information accurately, consistently and in a timely manner	• Record information in accordance with CCG policy and service specific procedures (see the Records Management Policy and any local procedures relevant to your work area). • You have a duty to maintain accurate records. (This is vital to the provision of services and the running of the CCG.) • If records are inaccurate, future decisions may be wrong and may result in harm to a service user or member of staff, and inefficient or ineffective use of resources. • If information is recorded inconsistently, information will be harder to interpret which may result in delays, possible errors or a lack of accountability. • If source data (including anonymised data), or the analysis and reporting carried out on it, is inaccurate, this may lead to the provision of services that do not meet the needs of the local population, or to inaccurate benchmarking.
6. Dispose of confidential waste appropriately	• Confidential information may be stored in a number of formats such as paper records, information in notepads/message books, CDs/DVDs, smartphones internal storage, USB memory sticks, tablets and other computers etc. • All such information and devices storing confidential information must be disposed of appropriately and in line with CCG policy, for example, use of 'confidential waste' boxes, shredding, destruction of hard drives etc. EMBED will securely dispose of electronic storage devices on behalf of the CCG.
7. Use confidential information in accordance with Sheffield CCG policies	• Be aware of all relevant CCG policies and procedures. An up to date list is available on the intranet. • Contact the Information Governance Lead for clarification of anything you do not understand.
8. Apply CCG policy within your sphere of influence	• Inform the staff you manage (or sponsor) what their responsibilities are in relation to information governance policies and what this means for them in their day to day work; for example, where to store information, acceptable email and internet use, not to share passwords or smartcards, what confidentiality means in practice, conditions for home working etc. • Ensure that service/team specific procedures are in place to implement CCG policy where required. • Ensure staff are appropriately trained in information governance relevant to their role. • Ensure information governance policy and process is adhered to and action taken to address non-compliance. • When staff leave, inform relevant people within the CCG so that their IT accounts/access to information systems can be disabled, ensure security passes, USB sticks, laptops, mobile phones etc. are returned.

9. Improve standards of practice wherever possible	It is not possible to achieve best practice overnight but we must work towards continuous improvement. In order to work towards achieving best practice staff must: • Be aware of the issues surrounding confidentiality, and seek training, support and advice as necessary in order to deal with them effectively. • Feedback comments or suggestions to managers on systems, procedures or working practices that give a cause for concern or could be improved. • Share good practice with colleagues (this is particularly important when poor practice is encountered). • Report breaches, suspected IG breaches and near misses (see s.10).
10. Report incidents and near misses in line with CCG policy	• Information governance incidents, including near misses, should be reported immediately in line with CCG policy. • The CCG is required to report serious IG incidents to supervisory authorities within 72 hours. • Information Governance incidents include but are not limited to: lost records or other information losses (for example, confidential personal or organisational information, business critical information), breaches of confidentiality, breaches of security, loss of IT equipment, inaccurate record keeping, sharing of passwords or smartcards, inappropriate use of information.

11. Use social networking media appropriately	Social computing includes but is not limited to: blogs, online discussion forums, collaborative spaces and media sharing services. Examples are Blogger, Instagram, Facebook and Twitter. These services are widely used and have many benefits. However, it is easy to inadvertently use them inappropriately. The communication is informal and with the many connections that are made between people it is easy to blur the boundary between work and personal life. As an informal method of communication it is easy to publish content that you may later regret and which may not be appropriate in a work context. Such information may end up having a much wider audience than you anticipated which cannot later be retracted. You should think carefully about what you publish even outside of work because inappropriate use could lead to disciplinary action. The use of social networking or blogging media at work, where you are representing the CCG in an official capacity requires prior approval. Care should be taken to use such media in a professional manner. (Contact the IT Department for technical support, for example, if access to a site is blocked but required in the course of your work.) Staff should take care to use social computing media, whether for work purposes or personal use, in a manner that is consistent with the terms and conditions of their employment or association with the CCG. For example, individuals should not post content that breaches confidentiality, contains inappropriate comments about colleagues, service users, or patients, is abusive or hateful, or would potentially cause embarrassment or detrimentally affect the reputation of the CCG. In addition, where appropriate, individuals should identify that any views expressed are their own and not those of their employer. Failure to adhere to such guidance may result in the individual being subject to disciplinary procedures. (See Internet Acceptable Use Policy)
Patient/Service User/Staff Rights	
12. Rights of individuals in relation to their information **(See also section 15, 16, 17, and 21)**	You should understand and respect the rights of individuals in relation to their information. Under the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR), individuals, known as data subjects, have certain rights about the way information about them is used. These include: • The right to be informed • The right of access • The right to rectification • The right to erasure

	• The right to restrict processing • The right to data portability • The right to object • Rights in relation to automated decision making and profiling. Detailed information on these rights is listed on the Information Commissioners website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/
Consent	
13. Consent to obtain information	• Inform patients/service users/staff about how we use their information and seek consent if appropriate. • Information collected for one purpose may not normally be used for another, incompatible, purpose without consent. • Where consent is being used for non-healthcare or non-statutory functions IG advice must be sought. • Please refer to Section 4 also.
14. Consent to use / share personal information	• Wherever possible, if personal information is to be shared it will be done with the **informed explicit consent** of the individual to whom it relates. • Informed consent is when an individual understands why their information is needed, how it will be used, who it will be shared with, the possible consequences of them agreeing or not to that proposed use, and gives consent. Informed consent may be explicit or implied, depending on the circumstances. (Ask the IG Lead for advice.) Explicit consent may be given orally or in writing. • Where a third party (such as the police, a solicitor or family member) requests access to records and has provided written consent of the individual, you should ensure that you are satisfied that the consent is informed. • You should inform patients, service users and staff that they generally have a right to object to the use and disclosure of confidential information that identifies them. • In certain circumstances, if a patient or service user chooses to prohibit the disclosure of information to other relevant professionals it may mean that the service that can be provided is limited or, in rare circumstances, cannot be provided at all. For example, assessments cannot be made and patients/service users treated safely and with continuity of care, without relevant information about their condition or medical history being shared appropriately. Complaints from patients and staff may not be able to be progressed unless certain information is shared with the person about whom the complaint has been made. • You must inform patients, service users and staff if their decisions about disclosure have implications for the provision of a service. • Where a patient or service user has been informed about the proposed uses and disclosures involved in the delivery

	of a service and their right to refuse permission, and they agree to their information being shared, then explicit consent is not required for each specific disclosure associated with that service. For example, the sharing of information within a multi-disciplinary team does not require explicit consent for each disclosure. • Even where there are grounds for sharing information without consent it is good practice to ask permission to share that information (unless it would prejudice the investigation of a crime or would put individuals at risk of harm). • Lack of consent should not prevent the sharing of information where there are concerns about the welfare of an individual. Disclosures without consent should only be done with appropriate authorisation (see section 15). • Following the introduction of the Health & Social Care (Safety and Quality) Act 2015, all staff have a duty to share non-sensitive personal data (e.g. names and addresses), where it is likely to help the provision of healthcare services to the patient and do not need explicit consent to do so.
15. Consent: capacity to consent (See also 12 and 17)	• Where an individual does not have the capacity to consent, the responsibility for deciding the appropriate course of action lies with the agency giving care or the person assigned Lasting Power of Attorney Health and Welfare (LPA) by the patient/service user. • Where the agency giving care is responsible for decisions about information sharing, these must be made in the best interests of the patient/service user taking into consideration any previously expressed views of the client. • In accordance with the Mental Capacity Act 2005 (MCA), the agency, where appropriate, should consult other people, especially: anyone previously named by the patient as someone who should be consulted, carers, close relatives or friends of the patient, any attorney appointed under the MCA, the views of an appointed independent mental capacity advocate (IMCA), any deputy appointed by the Court of Protection to make decisions for the patient.

16. Consent: children and young people **(See also 12 and 17)**	• Young people of 16 years and older are presumed to be competent to give their own consent. • In the case of children and young people under the age of 16, consent is usually required from one person with parental responsibility (who is usually the mother or father or someone who holds a court order giving them parental responsibility). • As children get older they gain rights for themselves. Children under the age of 16 can give consent for themselves if they have sufficient understanding and intelligence to fully understand what is proposed, that is, they are Gillick/Fraser competent (see section 12). • People with parental responsibility can authorise other people to make decisions about their children including the sharing of information.
Disclosing Personal Information	
17. Dealing with requests to access personal information (including access to the health records of deceased people) **(See also 15, 16 and 21))**	The Data Protection Act 2018 and the General Data Protection Regulation govern the personal information of living individuals (known as data subjects). Data subjects have a general right of access to **view or receive a copy of information** that is held about them. An individual can apply for access to his/her own information or authorise someone else to apply for access to this information on his/ her behalf (known as a subject access request). The CCG's Access to Records Procedure contains detailed instructions on handling such requests, including the following information: • Responses must be provided within one month. • The requester must provide sufficient information in order for the CCG to be able to locate the information and verify their identity. • Data subjects should be provided with an explanation of any information that is complex or unclear (e.g. abbreviations or technical terms). • They must also be informed of how their information is used and who it shared with. • Access to some or all of the information may be refused where it would cause serious harm or distress to the data subject or anyone else. All health information should be reviewed by an appropriate health professional prior to disclosure to determine if information should be withheld. Withholding information should be an uncommon event. Guidance must be sought from the Information Governance Lead if information is to be withheld. • Access to information that identifies another person will be normally refused unless they have consented to the disclosure, or it is reasonable to do so having considered the rights of all concerned. This does not apply to information concerning a health professional involved in the care of the individual and the information relates to care provided. Decisions to disclose or withhold information

	should be made on a case by case basis with advice sought from the IG Lead. • Consent to release information provided by a third party is not required. In certain cases it may be prudent however to discuss the request with the original provider of the information. Children and young people have a right to see information about themselves if they are regarded as 'Gillick / Fraser competent.[5] • People with parental responsibility can apply to see a child/young person's records but this will be refused if a child is deemed Gillick / Fraser competent and does not consent. <u>Records of Deceased Persons</u> • Requests to access the health records of deceased people can be made under the Access to Health Records Act 1990. Under this Act, the deceased's personal representative or anyone with a claim on the deceased's estate can request access to their records. • Where the deceased has previously made their wishes clear regarding access to their records, their wishes should be respected. • With regards to claims, only information relevant to the claim should be released. • The CCG's responses must be made within one month. • Decisions to disclose or withhold information should be made on a case by case basis, and advice should be sought from the Information Governance Lead.

[5] The underlying principle of the law is that for children under the age of 16 years parental rights yield to the child's right to make their own decisions when they reach a sufficient understanding and intelligence to enable them to understand fully what is proposed.

18. Reasons for disclosing information without consent **(See also 19, 20 and 21)**	• There are circumstances when it is necessary to share information even though the individual has not consented. • These circumstances are the exception rather than the rule. • Information can be shared without the consent of the person whom the information is about when: ∞ It is in the public interest to do so[6] ∞ It is required by law **Examples of sharing information in the public interest include:** • Where a child is believed to be at risk of harm (Children Act 1989). • Where there is a risk of harm to anyone including the data subject. • Where information is required for the prevention, detection or prosecution of a crime.[7] • Under the Mental Health Act 1983 where a service user objects to their 'nearest relative' being consulted re: - - An application for Treatment Order (Section 3) is being considered - An application for assessment and/or treatment in relation to the service user has been made. - Under the Mental Health Act (Patients in the Community) Act 1995 where the service user is known to have the propensity to violent or dangerous behaviour. • Domestic Violence, Crime and Victims Act 2004 gives victims of specified sexual or violent offences the right to be informed of certain decisions if the offender becomes subject to provisions under the Mental Health Act 1983. **Examples of sharing information where it is required by law include:** • Notification of certain infectious diseases • Where it is required by court order **Confidential information that is disclosed without consent must follow the appropriate process (see section 19, 20 and 21)**

[6] The public interest in sharing confidential information must be balanced against the public interest in maintaining a duty of confidentiality. Where that balance lies must be considered in each case, that is, the decision to disclose or withhold information must be made on a case by case basis.

[7] Disclosures of confidential information to the police without consent should normally be in relation to 'serious crime' only. Department of Health guidelines indicate that there is no clear definition of serious crime. Section 33 of the NHS Confidentiality Code of Practice (2003) states: "Murder, manslaughter, rape, treason, kidnapping, child abuse or other cases where individuals have suffered serious harm may all warrant breaching confidentiality. Serious harm to the security of the state or to public order or crimes that involve substantial financial gain or loss will generally fall within this category. In contrast, theft, fraud or damage to property where loss or damage is less substantial would not generally warrant breach of confidence.

19. Procedure for disclosing information without consent **(See also 17, 20 and 21)**	The appropriate procedure to follow must be decided on a case by case basis. • If it is felt necessary to share information where consent is withheld the individual should be informed of this decision (unless it would prejudice the investigation of a crime or would put individuals at risk of harm). It may be appropriate to give the individual an opportunity to disclose the information him/herself. • If it is not possible to obtain the consent of the individual, or it is not desirable, then the decision to share information should be taken at an appropriately senior level within the organisation. • The authority to disclose information may vary within different parts of the CCG and may depend on the reason for and/or circumstances of disclosure. It may lie with the Caldicott Guardian/SIRO/Information Governance Lead, or professional leads (for example, safeguarding). Requests requiring Caldicott approval should, unless there are exceptional circumstances, be routed via the Information Governance Lead, where such requests are made by the Police, UK Borders Agency or any other government agency, or where the information is required for research/analysis purposes, unless there are local procedures in place (for example, safeguarding). This is to ensure that all such requests are logged and the reason for decisions recorded centrally. • You should ask your line manager for the procedure you should follow or obtain advice from the Information Governance Lead. • It is a requirement of the CCG that the reasons for the final decision (either to share or not to share) must be recorded. • Where information is shared without consent the member of staff should document what information was released and when, to whom it was disclosed, and why it was felt justified. Likewise, it is important that decisions not to share information are also justified. Staff and/or the CCG can be held accountable for acts of omission as well as commission. • All non-consented disclosures must be reported to the Information Governance Lead for logging unless they are part of a delegated process, for example, Safeguarding Procedures.[8]

[8] Requests for information without consent, either of a victim or a perpetrator of crime, that fall outside of existing safeguarding processes such as medical notes, the date of next appointment at a drug treatment centre, a suspected perpetrator's address must be authorised by the Caldicott Guardian. These requests are logged and the reasoning for any decision recorded. This introduces a clear line of accountability to such decision making and allows information risk to be managed.

20. Procedure for disclosing information to the police **(See also 17, 18 and 19)**	• Requests for personal information from the police should be routed via the IG lead. • Requests should be in writing which can include faxes on headed paper and attachments from a personal police email account (i.e. *.pnn.police.uk). The identity of the requestor must be verified. • The request for information should specify why it is required and be countersigned by a senior officer of Inspector rank or above. (See section 18 for legitimate reasons for disclosing information without consent). • If it is not possible for the applicant to specify why the information is required (for example, because it would prejudice the investigation of a crime) then the request should be countersigned by a very senior officer of Superintendent rank or above • Information should only be disclosed with the proper authority (See section 19 and 21 (iv)). • Disclosures to the police may be very sensitive. Consider if special arrangements need to be put in place to facilitate disclosure, for example, the nomination of a specific member of staff to deal with the request. • Where police produce a consent form for the records they wish to access, a CCG member of staff should check with the data subject that the consent is informed. Staff should be mindful of the impact that sensitive information in a patient's record may have on the individual.
21. Check-list of points that must be considered before disclosing confidential information **(See also 17 and 19)**	(Refer to Access to Records Policy) The purpose of these questions is to help you decide the appropriate action to take if you are asked to disclose confidential information about a patient/member of staff. They are not sequential or definitive but are intended as a guide to good practice. i) Have I verified the applicant's identity? ii) Is there a legitimate reason for disclosing the information? iii) Is the information requested adequate, relevant and not excessive for the purpose? iv) Do I have the authority to disclose the information? v) What is the most appropriate method of disclosing the information? vi) Who do I need to inform that I have disclosed confidential information? vii) What do I need to record about the request and disclosure/non-disclosure? viii) Where do I record information about disclosure/non-disclosure? ix) Do I need to report the disclosure/non-disclosure to anyone?

i) Verifying identity	You must ensure that you can confirm the identity of the person and/or legitimacy of the organisation requesting information. You can verify identity in the following ways: ***Requests by the data subject or on behalf of the data subject*** If you are not familiar with the individual then you can ask for some photo identification and verification of address such as a utility bill. If the request is made on behalf of a data subject then proof of the relationship (for example, power of attorney, legal representative etc.) should be provided. **Request from another agency (for example, police, local authority)** ***Telephone requests*** Telephone the individual back via the main switchboard of their organisation (in addition, verify with switchboard if the person is employed there in their stated capacity). If you do not know the telephone number (for example, because it is an agency that you are not familiar with), then you should independently verify the number via a telephone directory/directory enquiry service; do not accept the number as given by the applicant. Unless there is a local procedure in place that states otherwise, you should ask for the request to be put in writing (which includes by fax or email attachments from a secure governmental email address). All requests from the police and other Government agencies should be put in writing. *Written requests* Written requests from organisations (for example, a solicitor or substance misuse agency) must be on headed notepaper. The address should be independently verified (that is, you should not accept an address/fax number given to you for an organisation that you are unfamiliar with). The identity of the applicant should be verified for all written requests.
ii) Legitimate reasons for disclosing information	1 The patient/service user/staff member wishes the information to be disclosed. 2 Disclosure is required by law, for example, by statute or court order. 3 The public interest in disclosing the information overrides the public interest in maintaining confidentiality. 4 Disclosure of the information is required for the purposes of providing care.

iii) Disclosing information that is adequate, relevant and not excessive for the purpose	Consider: 1. What does the recipient hope to achieve by the disclosure? (That is, what is the purpose of disclosing information?) 2. What is the minimum amount of information you can share to achieve that purpose? 3. Who does the information need to be shared with?
iv) Authority to disclose information – consented and non-consented disclosures including routine transfers of Personal confidential information (PCD)	Confidential personal or CCG information may only be disclosed with the proper authority and must be protected against improper disclosure at all times. Authority to disclose may be obtained from the patient/service user/staff member or from the designated individual in the CCG. ***Authority from the patient/service user/staff member*** The patient/service user/staff member has given authorisation for the disclosure of his/her information. ***Appropriate authority from within the CCG*** Disclosures of information that breach confidentiality should be authorised by the Caldicott Guardian/Senior Information Risk Owner/Information Governance Lead unless part of an authorised process such as safeguarding. (Advice can be obtained from the Information Governance Lead) All non-consented disclosures that fall outside of safeguarding or other local procedures should be reported to the Caldicott Guardian via the Information Governance Lead. All routine transfers of personal confidential information (PCD) must be authorised by the Information Governance Lead. All services should provide an up to date map of PCD flows to the Information Governance lead so that these flows can be risk assessed. This is a requirement of good information risk management and the Data Security and Protection Toolkit.
v) Appropriate methods of communicating ALL confidential information (including safe haven procedures) **(See also 22 – Safe Havens and Safe Haven Procedures)**	The most appropriate method of communicating information will depend on a number of factors including the sensitivity of the information, its destination and the urgency of the request. Information should be transferred effectively, that is, it should reach its destination in a timely manner, and securely. As a general rule, safe haven procedures must be followed (see 22). That is, you should inform the intended recipient that you will be sending them confidential information, you should agree on a secure method of transfer and you should request acknowledgment of its receipt. ***By post*** • Ensure you have an up to date address for the intended recipient. • Confidential information should be addressed to a named

	individual or team and marked 'Private and Confidential: for the addressee only'. • Confidential information sent in both the internal and external post should be in sealed envelopes or packaging and must include the full postal address. • Depending on the sensitivity of the information and where it is being sent to, information may be double or single wrapped and delivered by hand/ Royal Mail Special Delivery/ normal post/ internal post. Confidential information must not be transferred in a transit (internal mail) envelope whether it is sealed or unsealed. • Information sent through the internal post should contain the name of the service and the full work base address. • Information sent/transferred on portable media such as a DVD, CD rom or USB stick must be encrypted. ***By fax*** • It may not be appropriate to fax very sensitive confidential information. Recent advice to the NHS is not to transfer any personal confidential information by fax. Use of faxes within the CCG should be eliminated wherever possible. XXXref • Where it is necessary to fax confidential information, it should be faxed to a safe haven fax, where possible, using safe haven procedures. • A safe haven fax is one that is located in a separate office that has restricted access. • Confidential information can be sent to faxes situated in open plan offices by using safe haven procedures: The intended recipient should be telephoned and informed that you are about to send them confidential information. The intended recipient should wait by the fax machine and collect the fax immediately it arrives. The recipient should telephone you to let you know it has arrived. • Always fax information to a named recipient or team. • Routinely used numbers should be pre-programmed into the fax machine. • Faxed information going astray is usually down to user error so it is important to take care to enter the fax number accurately. If there is any doubt, a test fax can be sent followed by the confidential fax using the redial button. ***By telephone*** Ensure you know the identity of the caller before giving out information. (See 'verifying identity' above.) Do not leave confidential information on voicemail. ***By email*** Confidential information should not be shared by e-mail unless it is part of a work flow process agreed and authorised by the

	Information Governance Lead. Only encrypted transfers are permitted. Using [secure] in the subject field of all emails containing confidential information is mandatory and ensures emails are encrypted. The Email Policy contains further detailed guidance. Safe haven email procedures should be followed for particularly sensitive information.[9] **By text** Confidential or sensitive information must not be sent by SMS text message. **All routine flows of patient identifiable data should be mapped and a copy given to the Information Governance Lead. It is the responsibility of the Information Asset Owner to ensure that the information flow is mapped and risk assessed at least annually.**

[9] The sender should contact the intended recipient prior to sending the email to ensure it will be received in a timely manner, for example, to check the recipient is not on leave; the sender should check if any proxy access has been given to that account and whether it is appropriate to send the information in such circumstances; the sender should inform the recipient why the information is being sent and check that the information will be managed appropriately, for example, that it will be deleted from the email system; the recipient should be asked to confirm receipt of the email.

vi) Informing appropriate individuals that confidential information has been disclosed	***The patient/service user/staff member*** 1. Even where there are grounds for disclosing confidential information without consent it is good practice to ask permission to do so. However, the patient/service user/staff member should not be asked for permission to release information or told that information about them has been disclosed without their consent if it would prejudice the investigation of a crime or would put any individual at risk of harm. Not asking permission will be an exceptional event. 2. Where a patient/service user/staff member has disclosed information that you feel needs to be disclosed to a third party, it may be appropriate to give the patient/staff member an opportunity to disclose this information him/herself first. You should follow this up later, by an agreed date with the individual, to ensure the information has been disclosed. 3. If it is decided that it is necessary to disclose information even though the patient/service user/staff member has specifically withheld their consent, it is good practice to inform him/her of your intention (unless to do so would prejudice the investigation of a crime/result in harm – see point 1). ***Other individuals within the CCG or in other organisations*** 1. It is important to identify and inform any individuals who need to be made aware that confidential patient/service user/staff member information has been disclosed. This is particularly important where information has been disclosed without consent.
vii) Recording information about disclosures	All relevant information about disclosures must be recorded in the patient's notes/staff personal file or organisational folder. This includes: • The name of the person and agency making the request • The method of the request (telephone, in writing, by fax etc) • The purpose of the request • Whether information was disclosed or not • Who the information was disclosed to and by what method • Reasons for disclosure or non-disclosure • If there was consent to the disclosure or not (include reasons where consent was not obtained) • Who has been informed of the disclosure Disclosures that are reported to the Caldicott Guardian/Information Governance Lead are recorded and held in a central log.

22. Safe Havens and Safe Haven Procedures **(See also 26 and 21(v))**	Safe havens and safe haven procedures are associated with the secure transfer of patient information. There are two types: Accredited Safe Havens and Traditional Safe Havens, both of which are there to protect the security and confidentiality of information: • The **Accredited Safe Haven** and its associated processes relates to the storage, transfer and use of patient identifiable data that will be used primarily in a weakly pseudonymised or pseudonymised form for the purpose of non-direct care. Examples include: contract monitoring, performance monitoring, and the management and planning of services. The Health and Social Care Act 2012 impacted on the secondary use of identifiable data for management and planning of health services. As a temporary measure Accredited Safe Havens and Controlled Environments for Finance have been established under s251 of NHS Act 2006 to allow essential processes to continue. • The information processed in Accredited Safe Havens is subject to agreement with the HSCIC and strict guidelines laid down in the S251 approval. It will be used in identifiable form for non-direct care only when strictly necessary. (See the Head of Informatics). • **Traditional Safe Havens** and safe haven procedures refer to the secure transfer of patient identifiable information for operational purposes that are related to the direct health and social care of patients. For example, referrals for services. Historically relating to faxed information for invoicing, safe haven procedures should be used when transferring confidential information by whatever method unless there is a documented exception. • All ad hoc transfers must use safe haven procedures without exception. Safe haven procedures include informing the intended recipient that information is going to be transferred, checking the address (email or fax number) of the intended recipient and requesting confirmation that it has been received. • The sender should contact the intended recipient prior to sending the information to ensure it will be received in a timely manner, for example, to check the recipient is not on leave. • Where email is used, the sender should check if any proxy access has been given to the account and whether it is appropriate to send the information in such circumstances. The sender should inform the recipient why the information is being sent and check that the information will be managed appropriately, for example,

	where email is used, that it will be deleted from the email system. • A system for confirming receipt of the information should be put in place. This may be a direct request for confirmation from the recipient or a 'by exception' process where regular transfers of information are involved. That is, information is sent on a particular date and the intended recipient informs the sender if information is not received when expected. Non-receipt of information should be followed up and reported as incidents.
Information Security	
23. Use of Portable Devices	• This Section will be added when the "Remote Working & Portable Devices Policy" has been finalised.

24. Information Security (See also 21(v) and 26)	Personal information should be held, used and shared securely and confidentially and in line with CCG policies and procedures including the Information Security Policy. See guidance below:
24 (i) Confidentiality in public places	• Be aware of the difficulties of maintaining confidentiality in open plan offices. • Do not discuss confidential information in public areas where it may be overheard, for example: ~ In corridors ~ In reception areas ~ When using mobile phones • Do not record confidential information where it may be accessed by unauthorised people – for example, on post it notes, systems that are not protected by proper security, notice boards, card systems that are not locked away etc. • Do not work on confidential information in public places such as trains or coffee shops.
24 (ii) Access to information	• Do not browse electronic systems or records. • Do not access information which you do not have a need to know. • Save all information (confidential and non-confidential) on a secure server where available. • Ensure confidential information stored in a shared drive is accessible only to those with a need to know. • Consider how PC screens are positioned. Can confidential information be seen by anyone who does not have a need to know? • Do not leave confidential information unattended, for example, do not leave information out on your desk or leave your desk when you are logged onto information systems. • **Lock your PC** even when you are away from your desk for short periods such as to make a cup of tea or take a comfort break (Press the “Windows” key and ‘L’ simultaneously). • Share information on a need to know basis.

24 (iii) Information security	• Lock information away when not in use. • Confidential information not stored on a server, for example, information held on a PC or laptop hard drive must be encrypted and must be backed up regularly, kept in a secure place and transferred to a server at the earliest opportunity. • Portable devices should not be used to store personal confidential data without prior notification to the Information Governance lead in accordance with CCG policy (see section 23) • Do not install unauthorised software onto your PC laptop or smartphone. • Make sure your anti-virus software is up to date. • Virus check flash drives before introducing them onto your PC.
24 (iv) Send personal information appropriately (see 21(v))	• By post – to a named person or team in a sealed envelope marked 'Private and confidential: for the addressee only' • By fax – to a named person or team, include your contact details, use safe haven procedures, for example, telephone the recipient before faxing to ensure they are there to collect it (Consider if there it is appropriate to send information by fax - only use if a better alternative isn't available.) • By portable media – information must be encrypted and transferred appropriately • By telephone – ensure you know the identity of the caller before giving out information (See 21(i)) • Email – confidential information should not be shared by e-mail unless it is part of an authorised process (see Email Policy) • Don't leave confidential messages on voicemail • By text – Sensitive personal information should not be sent by SMS text message. It may be used to contact patients/clients, for example, to remind them of appointments. Texting should only be done with the consent of the individual concerned and be in line with CCG policy.The Information Governance Lead must be contacted prior to setting up such a system.

24 (v) Passwords	Use passwords to access electronic systems in line with CCG policy, for example, in deciding what the password should be, how often it is changed, not sharing passwords, locking workstations, password protecting documents etc. In particular: • Do not share passwords or smartcards with others • Change your password at regular intervals • Do no re-use old passwords • Do not write your passwords down in a way that would allow another to access it/use it to access your account • Avoid using short passwords or using names or words that are associated with you, for example, children's or pet's names • Use a combination of numbers, letters (upper and lower case) and characters • Do not allow others to use your smart card or share the pin number with anyone
25. Working from home **(See also 24 and 23)**	• Working from home should be in accordance with the CCG policy around home working, remote working and the use of portable devices • Confidential CCG information should not be placed on personally-owned equipment such as PCs, laptops, USB sticks, DVDs • Confidential information must not be placed on CCG provided portable media such as USB sticks and DVDs unless they are encrypted and the use has been authorised by line management.
Using data for secondary uses	
26. Rules regarding the use of patient identifiable information for non-direct care (secondary purposes) **(See also 22)**	• The Health and Social Care Act 2012 has introduced new restrictions on secondary use of identifiable data, national guidance and policy is evolving. • It is NHS policy and a legal requirement that person identifiable data can only be used for purposes not involving direct health care (that is, for secondary purposes) where there is a legal reason to do so. Legal reasons include patient consent or approval under section 251 of the NHS Act 2006. • If you are currently using patient identifiable data for the purposes of non-direct care, or you think you need to use patient data for non-direct care work, you must contact the Information Governance Lead for advice on what is now permissible.
Freedom of Information Act	

27. Freedom of Information Act, Environmental Information Regulations and requests for information **(See also 17)**	Under the Freedom of Information Act 2000 (FOI), individuals can write (including by fax or email) and request access to any information public bodies hold. Under the Environmental Information Regulations 2004 (EIR), requests to public bodies for environmental information do not have to be made in writing. The CCG is subject to FOI or EIR so staff need to know how to recognise and handle such requests. Public bodies are legally obliged to provide a response to a FOI request, including any disclosable information, within 20 working days. All requests for information that reference FOI and EIR should be sent to the FOI administrator for logging. The FOI administrator will ensure the request is passed to the correct department and/or co-ordinate the response. If you receive a request or you are asked to respond to a request, you must deal with it in a timely manner to ensure the organisation is able to gather information and approve the request in compliance with the legal timeframe. Information may be withheld if it falls within one of the specified exemptions in the FOI Act (known as exceptions in the Regulations). This includes information that is confidential (relating to the CCG, a partner organisation or an individual), or if it would prejudice anyone's commercial interests. If the CCG withholds information, the applicant must be provided with an explanation (known as a refusal notice). That is, **ALL** applicants must receive a response regardless of whether they are provided with any information or not. Applicants do not have to state that they are making the request under FOI or EIR so theoretically any request for information may be a request under either of these pieces of legislation. To avoid being overly bureaucratic only certain requests should be dealt with under FOI or EIR. The process for dealing with requests for information is: • Respond to routine requests as normal in a timely manner • FOI or EIR requests should be sent to the FOI administrator. • A request that falls under the CCG FOI or EIR process is one which: ~ Specifically refers to Freedom of Information or Environmental Regulations ~ Requires a **Co-ordinated response** ~ Is **Complex** and will take a significant amount of time or effort to compile a response (this enables us to monitor the amount of time that FOI and EIR requests are taking) ~ Is **Contentious** (for example, the response may be about a sensitive issue in the news, you think the information may be exempt from disclosure)

Freedom of Information Act, Environmental Information Regulations and requests for information (continued) **(See also 17)**	• Deal with all requests for information promptly: Legislation requires that responses are sent to the applicant within 20 working days • If you are asked to respond to a FOI or EIR request and think an exemption or exception may apply, you should contact the CCG's FOI Administrator for guidance. **All exemptions or exceptions** are applied by the Chief of Corporate Affairs. • A request from an individual for information that the CCG holds about applicant which references the Freedom of Information Act (FOI) will be exempt under FOI but should be dealt with under the Data Protection Act 2018/GDPR and a response given within one month.

5 Monitoring effectiveness of the policy/procedural document

All staff should have a workplace induction that raises awareness of service specific information governance issues.

All staff need to complete information governance training annually
Key staff need to complete specified information governance modules (provided via the IG Training Tool electronically)

6 Review

Review date: November 2020

This document may be reviewed at any time at the request of either staff will automatically be reviewed after 12 months and thereafter on a bi-annual basis or when a change in legislation dictates.

7 References and links to other documents

NHS Confidentiality Code of Practice
Records Management Policy
Data Protection Act 2018 (DPA)
General Data Protection Regulation (GDPR)
The Health and Social Care Act 2012
Health & Social Care (Safety and Quality) Act 2015
Health Records Act 1990
Children Act 1989)
Mental Health Act (Patients in the Community) Act 1995
Remote Working & Portable Devices Policy
Section 251 of the NHS Act 2006
Under the Freedom of Information Act 2000 (FOI)
Environmental Information Regulations 2004 (EIR),

8 Equality and Diversity Statement

NHS Sheffield CCG aims to design and implement services, policies and measures that meet the diverse needs of our service population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the Human Rights Act 1998 and promotes equal opportunities for all. This document has been assessed to ensure that no-one receives less favourable treatment on grounds of their gender, sexual orientation, marital status, race, religion, age, ethnic origin, nationality, or disability. Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the person requesting has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.

NHS Sheffield CCG embraces the six staff pledges in the NHS Constitution. This policy is consistent with these pledges.

9 Disability Confident

NHS Sheffield CCG has been accredited with the Disability Confident Award – level 1. This is in recognition of meeting the commitments regarding employment of disabled people and permits the organisation to use the Disability Confident logo on all of its stationery. The Disability Confident symbol should be added as afooter to all policies / procedural documents.

NHS Sheffield Clinical Commissioning Group

NHS Sheffield CCG Equality Impact Assessment 2016

Equality Impact Assessment

Title of policy or service:	Confidentiality Code of Conduct and Data Protection Policy	
Name and role of officer/s completing the assessment:	Sandie Buchan, Head of Information, Performance & PMO (Sheffield CCG) Gershon Nubour, Information Governance Manager (eMBED)	
Date of assessment:	5th November 2018	
Type of EIA completed:	**Initial EIA 'Screening'** ☐ ***or*** **'Full' EIA process** ✓	

1. Outline	
Give a brief summary of your policy or service • Aims • Objectives • Links to other policies, including partners, national or regional	To provide a formal structure and framework for how the organisation complies with its Information Governance obligations in relation to working with confidential information and promoting it throughout the organisation. Links to other policies are within the policy

Identifying impact:

- **Positive Impact:** will actively promote or improve equality of opportunity;
- **Neutral Impact:** where there are no notable consequences for any group;

- **Negative Impact:** negative or adverse impact causes disadvantage or exclusion. If such an impact is identified, the EIA should ensure, that as far as possible, it is justified, eliminated, minimised or counter balanced by other measures. This may result in a 'full' EIA process.

2. Gathering of Information
This is the core of the analysis; what information do you have that might *impact on protected groups, with consideration of the General Equality Duty*.

	What key impact have you identified?			For impact identified (either positive an or negative) give details below:	
(Please complete each area)	**Positive Impact**	**Neutral impact**	**Negative impact**	**How does this impact and what action, if any, do you need to take to address these issues?**	**What difference will this make?**
Human rights	x	x	☐		
Age	☐	x	☐		
Carers	☐	x	☐		
Disability	☐	x	☐		
Sex	☐	x	☐		
Race	☐	x	☐		
Religion or belief	☐	x	☐		
Sexual orientation	☐	x	☐		
Gender reassignment	☐	x	☐		
Pregnancy and maternity	☐	x	☐		
Marriage and civil partnership (only eliminating discrimination)	☐	x	☐		
Other relevant groups	☐	x	☐		
HR Policies only: Part or Fixed term staff	☐	x	☐		

IMPORTANT NOTE: *If any of the above results in '**negative'** impact, a 'full' EIA which covers a more in depth analysis on areas/groups impacted must be considered and may need to be carried out.*

Having detailed the actions you need to take please transfer them to onto the action plan below.

3. Action plan				
Issues/impact identified	**Actions required**	**How will you measure impact/progress**	**Timescale**	**Officer responsible**

4. Monitoring, Review and Publication				
When will the proposal be reviewed and by whom?	**Lead / Reviewing Officer:**	**Information Governance Manager (eMBED)** **Information Governance Group (Sheffield CCG)**	**Date of next Review:**	**November 2020**