

# Information Access Policy

IG04



## Contents

1. Introduction.....	3
3. Information Access Requests.....	8
4. Duties and responsibilities.....	19
5. Implementation.....	21
6. Training Implications.....	21
7. Related Documents.....	21
8. Monitoring, review and archiving.....	22
9. Equality analysis.....	23
Appendix A: Summary of Key Legislation.....	27

### Version Control

Version	Date Approved	Committee	Date of next review	CCG Lead
2	1 March 2016	Executive Committee	January 2018	Deborah Cornell
2.1	April 2018	Executive Committee	May 2018	Deborah Cornell
3	July 2018	Executive Committee	July 2020	Deborah Cornell

## 1. Introduction

The CCG aspires to the highest standards of corporate behaviour and clinical competence, to ensure that safe, fair and equitable procedures are applied to all organisational transactions, including relationships with patients their carers, public, staff, stakeholders and the use of public resources. In order to provide clear and consistent guidance, the CCG will develop documents to fulfil all statutory, organisational and best practice requirements and support the principles of equal opportunity for all.

This policy relates to all information and records held by or on behalf of the CCG whether computerised, paper or any other permanent storage media, including photographic, video and voice recordings and is supported by appropriate procedures to assist staff in complying with the CCG's statutory obligations. This policy will be available on the internet in line with the guide to information.

The information access regime or 'right to know' is governed by a range of legislative provisions detailing the circumstances in which individuals are entitled to obtain information from public bodies.

This policy is specific to providing information in response to access requests; it supports but does not prevent the CCG from answering questions from patients, service users, partners and the public as they arise during the course of normal business activities.

This policy supports and enables the principle that openness and not secrecy should be the norm in public life. Individuals have a right to privacy and confidentiality; this policy does not overturn the common law duties of confidentiality or statutory provisions that prevent disclosure of personal information about individuals.

Although there are variations in the application of the strands of legislation, the general starting point is that information should be provided to the requestor in a timely manner, in their preferred format and in full, unless there is a very good reason to withhold some or all of the information requested.

As requestors need not mention the relevant legislation, there are tight statutory timescales for responding, and penalties for failure to comply, it is essential that all staff across the CCG can identify an information access request on receipt to ensure that it is passed to the appropriate department for processing.

Responding to requests may involve gathering information from a range of sources and it is essential that staff and managers understand the importance of providing relevant information in a timely manner to ensure that the CCG complies with its statutory obligations.

**NB:** The European Union General Data Protection regulation (GDPR) which was adopted by the European Union in 2016, came into force in all EU member states on 25 May 2018. GDPR is incorporated into and supplements the UK Data Protection Act 2018.

## 1.1 Status

This policy is an information governance policy.

## 1.2 Purpose and scope

It is the duty of each NHS body to establish and keep in place arrangements for the purpose of monitoring and improving the quality of healthcare provided by and for that body. The CCG is committed to this policy and its implementation.

This policy applies to all members of staff employed by the CCG regardless of the type of contract which they hold. This policy also applies to agency and contract staff working on CCG business.

This document sets out the information access request process for the CCG and explains the framework for responding to requests for information under statutory access regimes, including:

- Freedom of Information Act 2000 (FOIA)
- Environmental Information Regulations 2004 (EIR)
- Data Protection Act 2018 (DPA)
- General Data Protection Regulations 2016
- Access to Health Records Act 1990 (AHRA)

This policy underpins all operational policies, procedures and activities connected with the implementation of the legislation and sets out the general principles with reference to:

- Responding to requests for information
- Responding to subject rights requests under the DPA 2018;
- Providing advice and assistance
- Application of exemptions or exceptions;
- Consultation with third parties
- Refusal or part refusal of requests
- Complaints about responses to requests for information
- Recording and monitoring requests for information.

It provides staff and the public with assurance about the CCG's commitment to openness and accountability balanced with the duty of confidentiality owed to individuals.

## 2. **Definitions**

This is a descriptive list of the definitions of terms used throughout this policy:

- 2.1 Personal information: is factual information or expressions of opinion which relate to an individual who can be identified from that information or in conjunction with any other information coming into possession of the data holder. This also includes information gleaned from a professional opinion, which may rely on other information obtained.

Personal information includes name, address, date of birth or any other unique identifiers such as NHS number, hospital number and national insurance number.. It also includes information which, when presented in combination, may identify an individual e.g. postcode, date of birth etc.

The DPA 2018 defines personal data as 'any information relating to an identified or identifiable individual'. Identifiable living individual is defined as 'a living individual who can be identified, directly or indirectly, in particular by reference to

- a) an identifier such as a name, an identification number, location data or an online identifier, or
- b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual'.

2.2 Sensitive Personal Data: also known as 'special category data' as set out in the DPA 2018 is any information about a person relating to their;

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade union membership
- Biometric Data
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence, or
- Any proceedings for any offence committed or alleged to have been committed

2.3 Health/social care records: contain information about the physical or mental health and/or social care of an identifiable individual made by or on behalf of a health or social care professional and in connection with the care of that individual, regardless of whether held electronically, on paper or any other media.

The DPA 2018 defines a health record as 'a record which consists of data concerning health and has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates'. It does not define a social care record.

2.4 Corporate information: is held in corporate records which relate to the business of the CCG such as accounts, minutes and meeting papers, contracts, legal and other administrative documents.

2.5 Requestor: is the person making the request for information, whether that is the person whose personal information it is or another third party, or someone requesting corporate information.

2.6 Subject access rRequest: is the term used in the Data Protection Act for a request by a living individual (or his/her representative) to view and/or receive a copy of their own personal information held on computer or in certain paper records.

2.7 Subject Rights Request: The DPA and GDPR extend the rights of data subjects who now also have the right to have their data; amended, erased, transferred to another organisation (known as data portability), or to have the processing of their

data altered or stopped. Some exemptions apply to health records but requests to do any of the above should be treated with the same level of importance and timescales as a Subject Access Request.

- 2.8 Third Parties: a third party is an individual other than the requestor or any external organisation or company other than the CCG. This includes family members of an individual; legal representatives; contractors working for and partner organisations working with the CCG.
- 2.9 Re-use of Information: means the use by any person or organisation of a document, record or information held by the CCG for a purpose other than the initial purpose which it was produced. This could include, for example, research purposes or combining the information with information from other public bodies for comparison or publication. Under the Data Protection Act 2018 we must be clear about what our purposes for processing are from the start. We must record our purposes as part of our documentation obligations and specify them in our privacy information for individuals. We can only use personal data for a new purpose if this is; compatible with the original purpose, we get consent, or we have a clear basis in law.
- 2.10 Redact: means removing exempted information from a document or record before responding to a request. This includes editing a document, blanking out specific information, or extracting non-exempt information and retyping into a new document.
- 2.11 Information Commissioner: is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The GDPR refers to a “supervisory authority” in EU member states – in the UK the Information Commissioner is the supervisory authority.

- 2.12 Solicitor: is someone with the legal authority (registered with the Office of the Public Guardian) to act on behalf of and in the best interests of another individual in relation to their welfare, wellbeing, money and/or property.
- 2.13 Data: Information which; (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should be processed by means of such equipment; (c) is recorded as part of a relevant filing system; (d) does not fall within any of the above, but forms part of an accessible record; (e) is recorded information held by a public authority and does not fall into paragraphs a to d.
- 2.14 Accessible record: (a) a health record; (b) an educational record; (c) an accessible public record.

The DPA 2018 defines a health record as, “a record which consists of data concerning health and has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates”.

- 2.15 Processing: Processing in relation to personal information means; obtaining, recording, holding or deleting information.

The DPA 2018 defines processing as ‘an operation or set of operations which is performed on personal data, or on sets of personal data, such as

- a) collection, recording, organisation, structuring or storage
- b) adaption or alteration
- c) retrieval, consultation or use
- d) disclosure by transmission, dissemination or otherwise making available
- e) alignment or combination, or
- f) restriction, erasure or destruction’.

2.16 Data processor: Any person, other than an employee of the data controller, who processes information on behalf of the data controller.

In GDPR Processor is defined as, “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data”. The DPA 2018 replicates this.

2.17 Data subject: A living individual who is the subject of personal data / information.

The DPA 2018 defines data subject as ‘the identified or identifiable living individual to whom personal data relates’.

2.18 Data controller: A person who either alone, jointly or in common with other persons, determines the purposes for which and the manner in which any personal data are, or are to be processed.

The GDPR and draft UK Data Protection Bill do not define data controller. In the GDPR, the data controller is defined as ‘the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data’. The DPA 2018 replicates this.

2.19 Recipient: Any person to whom personal data are disclosed.

The GDPR defines a recipient as ‘natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. The DPA 2018 defines recipient as ‘any person to whom the data is disclosed, whether a third party or not, but it does not include a public authority to whom disclosure is or may be made in the framework of a particular inquiry in accordance with the law’.

2.20 Absolute exemption: Information that does not have to be released to an applicant either through the publication scheme or in response to a request for information.

2.21 Qualified exemption: Information to which an exemption applies that requires the public authority to take a test of prejudice or to demonstrate that the balance of public interest is in favour of non-disclosure.

2.22 Applicant: Individual(s) or trust requesting access to information under the FOIA.

2.23 Duty to confirm or deny: Duty of the public authority to provide information as to whether it holds information specified in a request.

- 2.24 Fees notice: Written notification issued to an applicant stating that a fee for release of the requested information is payable. Fees are no longer allowed for Subject Access Requests and Subject Rights Requests unless the request is manifestly unfounded or excessive.
- 2.25 Fee regulations: National regulations that prohibit a fee with regard to certain types of information, and set the limit at which an organisation may charge for the provision of information.
- 2.26 General right of access: Section 1 of the FOIA confers a general right of access to information held by public authorities. An applicant has the right to be told whether the authority holds information requested, and be provide an copy of the information unless an exemption applies
- 2.27 Lord Chancellor's department: Government department responsible for the efficient administration of justice in England and Wales.
- 2.28 Publication scheme: Scheme specifying the classes of information which a public authority publishes or intends to publish.

### **3. Information Access Requests**

The CCG may receive information access requests in a variety of ways and the procedures to follow for responses, including potential charges, exemptions and timescales, vary depending upon which legislation is relevant to the information requested.

It is essential that the CCG identifies the correct legislation on receipt of the request, especially as the requestor is not required to mention the legislation, may quote the wrong legislation or the request may include information falling under more than one Act.

The CCG may occasionally choose to provide additional information outside the legislative framework at its discretion and without obligation.

Although information access requests under FOIA and DPA must be made in writing, this may cause difficulties for some requestors due to, for example, communication issues or disability, and therefore the CCG will provide advice and assistance to enable equality of access for all.

The GDPR and DPA 2018 do not require a request to be made in writing.

#### **3.1 Freedom of Information Act (FOIA)**

##### **3.1.1 *Published information***

Under the FOIA, all public authorities are obliged to adopt and maintain an approved publication scheme.

The CCG's publication scheme is available on the website detailing the information that it has published and that it intends to publish in the future, including the format

in which the information is available with links to specific documents where possible.

Requests for published information detailed in the scheme may be made verbally or in writing and will be dealt with in the normal course of business, by referring the requestor to the appropriate webpage or providing a printed copy.

The contents of the scheme will be regularly reviewed and updated and, if the CCG regularly receives requests for similar or specific categories of unpublished information, it will consider pro-actively publishing these in the scheme in future.

### 3.1.2 Unpublished information

Requests for unpublished information must be made in writing, including the requestor's name, with a postal or email address for response, and a description of the information being requested. There is no requirement for the requestor to mention the FOIA in the request or to prove their identity. They are also not required to state why they require the information or the purpose of their request, although this can assist in identifying the information requested.

If a request is phrased in too general a manner, the requestor can be asked for clarification and the CCG will offer advice and assistance for them to do so. If the request is still too general, the CCG may be unable to answer it.

Requests can come from any individual or organisation worldwide.

## 3.2 Environmental Information Regulations 2004 (EIR)

3.2.1 As with FOIA, requests for published information may be made verbally or in writing and will be dealt with in the normal course of business.

3.2.2 However, requests for unpublished information under the EIR do not have to be in writing as the information access request can also be made by telephone or in person. As the request can arise during the course of normal conversation, this can cause difficulties in identifying and responding to a request.

3.2.3 If a request is phrased in too general a manner, the requestor can be asked for clarification and if the request is still too general, the CCG may be unable to answer it.

3.2.4 Requests can come from any individual or organisation worldwide.

## 3.3 Data Protection Act 2018 (DPA)

### 3.3.1 By individuals

Subject access requests for personal information under the DPA must be made in writing by the living individual concerned or his/her representative. The request must include evidence of identity, the required fee in line with the CCG's current published schedule of charges, enough information to locate the relevant files or records and, in the case of a representative, evidence of authority to act.

The GDPR and draft UK Data Protection Bill does not require a request to be made in writing.

Information access requests are most likely to come from patients, service users, staff and contractors. These can only be accepted from the individual concerned; his/her authorised representative; an adult with parental responsibilities (in the case of children under the age of 13 or not yet competent to make their own decisions); a solicitor with authority to manage the affairs of an individual with or without the mental capacity to manage their own affairs; and any person appointed by the Court of Protection to act on behalf of an individual without the mental capacity to manage their own affairs.

Family members and friends who do not meet these conditions are not entitled to access the personal information of others and, although they may request access, this is likely to be denied on the grounds of confidentiality in all but exceptional cases.

### 3.3.2 By third parties

The CCG will not generally disclose personal information about living or deceased individuals in compliance with the requirements of DPA and the common law duty of confidence.

There will be occasions however when the CCG receives a request for personal information from third parties and may disclose some or all of the information requested with or without the knowledge of the individual concerned.

Such disclosures may take place because it is a legal requirement, for example under a court order, or specific information about a health or social care worker required under the Health Professions Order 2001 for the investigation of 'fitness to practice' or required by a coroner in relation to an unexpected or suspicious death.

Other investigatory bodies may also request information, including the Police and Revenue and Customs (HMRC). They must provide the CCG with a written explanation of why the information is required and the likely effect on investigation or prosecution if it is not provided. The CCG is not obliged to disclose personal information in these circumstances and will take account of all the relevant factors before reaching a decision about whether and how much to disclose.

The crime and taxation restrictions in the DPA 2018 replicate section 29 of the 1998 Act.

Unless third parties have a court order for original documents, all information disclosed will be copies or retyped extracts from files and records.

Specific guidance for staff is available and a complete record of the information access request, the decision process and outcome will be kept to ensure that disclosures can be justified if necessary to the Information Commissioner and/or the individual concerned.

### 3.4 Access to Health Records Act 1990 (AHRA)

- 3.4.1 Requests for access to information in the health records of deceased individuals may be made verbally or in writing.
- 3.4.2 Requests can only be accepted from the deceased patient's personal representative (the executor of the will/estate dealing with probate) and/or from individuals with a claim arising from the death.
- 3.4.3 Family members and friends who do not meet the specific criteria in the legislation are not entitled to access the health record and, although they may request access, this is likely to be denied on the grounds of confidentiality in all but exceptional cases.
- 3.4.4 The AHRA relates specifically to health records and there is no equivalent legislation allowing access to the social care records of deceased service users. The CCG will consider information access requests but is likely to deny requests on the grounds of confidentiality in all but exceptional cases.
- 3.4.5 The CCG may disclose information about the health or social care of the deceased that is already in the public domain, for example information considered at an inquest or coroner's court or recorded on the death certificate.

### 3.5 Responding to Requests

All information access requests will be responded to in line with legislative requirements for timeliness and completeness and in accordance with the CCG's procedures current at the time of receipt of the request.

The CCG's default position is to release the information requested unless there is a very good or legal reason not to do so. Occasionally a refusal notice may be issued as detailed in section 9.6 below rather than by providing some or all of the information requested.

Information will be provided in the format specified by the requestor whenever reasonably practicable. If it is not possible to provide information in the preferred format, an explanation will be given as to the reason why. Where appropriate the CCG may offer the option to view the relevant information or record, rather than providing a permanent copy, however there is a legal duty to facilitate a request and provide information in the format that the recipient has asked for.

The option to view is not included in GDPR and the DPA 2018.

The CCG will explain the appeals and complaints process in its responses.

#### 3.5.1 Freedom of Information Act 2000 (FOIA)

Responses to information access requests under FOIA will be issued promptly and not later than 20 working days from receipt.

The only exceptions will be when consideration is being given to the public interest test regarding the applicability of any qualified exemptions. The requestor will be informed of the reason for delay and the expected response date within 20 working

days of receipt of the original request. Where the request is not clear or could be interpreted in more than one way, clarification will be sought from the requestor before responding. Where charges are applicable, a fees notice will be issued to the requestor.

The time between issuing the fees notice and receiving payment is not included in the 20 working day response period. If the fees are not paid within three months, the information access request will lapse.

### 3.5.2 Environmental Information Regulations 2004 (EIR)

Responses to information access requests under EIR will be issued promptly and not later than 20 working days from receipt.

The only exceptions will be where the request is particularly complex or involves providing large amounts of information. The requestor must be informed within 20 working days as to whether the time for response must be extended or refuse the request as impractical and offer advice and assistance to reduce the scope of the request to more manageable proportions.

If charges are applicable, a fees notice will be issued to the requestor asking whether they wish to proceed with all or part of the information access request and offering advice and assistance to modify the request and reduce the fees charged. The time between issuing the fees notice and receiving payment is not included in the 20 working day response period. If the fees are not paid within 60 working days the information access request will lapse.

### 3.5.3 Data Protection Act 2018 (DPA)

Responses to subject access requests under DPA will be issued promptly and not later than 1 month (30 calendar days) from proof of identity.

An extension of 2 months (60 calendar days) can be used where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

The only exception will be if producing a copy of the personal information in permanent form would involve disproportionate effort. In such instances, the CCG will explore other more practical options for responding with the requestor.

### 3.5.4 Access to Health Records Act 1990 (AHRA)

Responses to information access requests under AHRA will be issued promptly and not later than:

- 21 calendar days from receipt for records which have been added to in the preceding 40 days
- 40 calendar days for all other records, subject to payment of relevant charges.

The CCG will only provide the personal representative (the executor of the will/estate dealing with probate) with partial or full access to the health records of deceased patients as required for that purpose.

The CCG will only provide individuals with a claim arising from the death with access to the parts of the health records of deceased patients relating to the cause of death and/or final illness as relevant to pursuing the claim.

### 3.6 Exemptions, Exceptions, Refusal or Part Refusal

The CCG will consider application of the relevant exemptions and exceptions against information access requests on a case by case basis, and will only withhold information if it can be justified.

Where only part of a document, record or other information is exempt, this information will be removed or redacted and the remainder of the requested information will be provided.

The CCG will issue an appropriate refusal notice to requestors when it is refusing to respond outright to an information access request, or for any information that is wholly or partly withheld under any exemption or exception.

#### 3.6.1 Freedom of Information Act 2000 (FOIA)

There are 23 exemptions to disclosure under FOIA but not all are applicable to the functions of the CCG. For example, information that is exempt due to national security, international relations or communications with the Royal household.

Of the exemptions that may be applicable some are absolute (e.g. disclosures prohibited by law, or information provided in confidence, or personal information where disclosure may contravene the data protection law), the CCG will not disclose information that is covered by an absolute exemption, and may choose to 'neither confirm nor deny' the existence of the information.

Other exemptions are qualified and subject to the 'public interest test', for example information affecting commercial interests, relating to legal professional privilege, intended for future publication, or prejudicial to effective conduct of public affairs. Qualified information will only be disclosed if, on balance, the public interest in disclosing exempted information is equal to or greater than the public interest in withholding.

The CCG can refuse to provide information where it is estimated that the cost of processing the request exceeds the appropriate limit, currently £450 based on 18 hours at £25 per hour to locate and retrieve the information. The refusal notice will explain how the cost has been calculated and offer the requestor advice and assistance to modify their request to enable a response below the cost limit.

The CCG can also refuse a request that is a repetition of a previous request or that is considered as vexatious.

If the CCG withholds some or all of the information requested, a refusal notice will be explaining what exemption has been applied and why, the public interest considerations that have been taken into account (where applicable), the internal review process and the requestor's right to complain to the Information Commissioner.

### 3.6.2 Environmental Information Regulations 2004 (EIR)

Information may be withheld under one or more of the exceptions if disclosure relates to internal communications or would adversely affect:

- International relations, defence, national security or public safety;
- the ability of a person to receive a fair trial, or a public authority to conduct an inquiry of a criminal or disciplinary nature;
- intellectual property rights;
- confidentiality proceedings of the authority;
- confidentiality of commercial or industrial information;
- the interests of any person who provided information voluntarily and has not consented to its disclosure;
- the protection of the environment to which the information relates.

These exceptions are not absolute, but are all subject to the 'public interest test'. The CCG will disclose information if, on balance, the public interest in disclosing accepted information is equal to or greater than the public interest in withholding.

A request may be refused if it is manifestly unreasonable or too general, but advice and assistance should be provided to make the request more manageable. Requests relating to unfinished documents or data can also be refused, although the requestor must be informed when the information is expected to become available.

If the CCG withholds some or all of the information requested based on application of exceptions, it will issue a refusal notice explaining what exception it has applied and why; the public interest considerations taken into account; the internal review process; the requestor's right to complain to the Information Commissioner.

### 3.6.3 Data Protection Act 1998 (DPA)

Personal information may be withheld under the DPA if, in the opinion of a health or social care professional, disclosure would be likely to cause serious harm to the physical or mental health of the requestor or to any other individual; the information includes personal information about a third party who has not consented to disclosure; disclosure would be likely to affect the CCG's ability to bring or defend legal proceedings; disclosure would be likely to affect the prevention or detection of crime.

The CCG is not required to respond to repeated subject access requests unless a reasonable period of time has elapsed and/or the personal information is likely to have changed since the last request.

If information is withheld based on an exemption, a refusal notice will be explaining: what exemption it has applied and why, the internal review process and the requestor's right to complain to the Information Commissioner.

**NB:** In the GDPR and UK Data Protection Bill, as with the DPA subject access rights are not absolute and requests may be refused wholly or in part. The serious harm test is carried over into the UK Bill for health records.

### 3.6.4 Access to Health Records Act 1990 (AHRA)

There are few exemptions in the AHRA because access to the health records of deceased patients is limited to certain individuals for specified purposes.

The health records of a deceased patient are exempt from disclosure in full if there is a note on the record, made at the request of the patient, that s/he did not want access to be granted for such a request or to a particular requestor.

Information held in the health records of a deceased patient is exempt in part if, in the opinion of the record holder, it is information likely to cause serious harm to the physical or mental health of any person; it is information relating to or provided by anyone other than the patient who could be identified from that information, unless the third party is a health worker or has consented to disclosure; in the opinion of the record holder, it would disclose information provided by the patient in the expectation that it would not be disclosed; the information was obtained as a result of an examination or investigation to which the patient consented in the expectation it would not be disclosed.

If the CCG withholds information based on an exemption, a refusal notice will be issued explaining what exemption it has applied and why, the the internal review process and the requestor's right to complain to the Parliamentary and Health Service Ombudsman.

### 3.7 Transferring Requests for Information

3.7.1 If the CCG receives a request for information which it does not hold (or holds only in part) but which it knows or believes is held by another public authority, then it will consider what would be the most helpful way of assisting the requestor in line with the FOIA and EIR codes of practice.

3.7.2 Depending on the circumstances, this is likely to involve providing any information that it does hold under FOIA or EIR at the earliest opportunity, informing the requestor that the information may be held by another public authority. The requestor should also be provided with contact details for that authority with the suggestion to reapply to that authority. If the requestor indicates that they do not object to the transfer of the request to the other public authority, then the CCG may transfer the request directly and notify the requestor this has been done.

3.7.3 The time for compliance in respect of information not held by the CCG does not start until the request is received by the public authority that does hold it.

3.7.4 The CCG will not transfer requests for personal or health information received under DPA or AHRA due to confidentiality requirements, unless the requestor specifically consents to the transfer or it forms part of a specific Subjects Rights Request for data portability, but will assist to identify the public authority most likely to hold their information.

### 3.8 Consultation with Third Parties

3.8.1 The CCG may hold substantial information provided by, obtained from or relating to third parties, for example in relation to contracts or joint working with other organisations.

3.8.2 The CCG will only accept information from third parties in confidence if it is necessary to obtain that information in connection with the exercise of any of its functions and it would not be otherwise provided, and will not agree to hold information 'in confidence' which is not truly confidential in nature.

3.8.3 In addition, information that is confidential at the time of acceptance by the CCG may no longer be confidential at the time of an information access request due to the passage of time or having already entered the public domain.

### 3.9 Contracts

3.9.1 When entering into contracts, the CCG will refuse contractual terms which seek to restrict the disclosure of information relating to the contract beyond those restrictions permitted by law. Unless a legal exemption is applicable in relation to any particular information, the CCG will be obliged to disclose in response to an information access request regardless of the terms of the contract.

3.9.2 In exceptional circumstances the CCG may agree to include non-disclosure provisions in a contract by means of a schedule which clearly identifies the information that should not be disclosed. The CCG will ensure when drawing up any such schedule that the contractor understands restrictions on disclosure could potentially be overridden by its legal obligations to respond to information access requests.

### 3.10 Partner Organisations

3.10.1 Before disclosing any information obtained from other organisations or through joint working, the CCG will consult with those organisations to take account of the potential effect that disclosure may have on the functions of third party partner organisations.

3.10.2 However, the final decision about disclosure and/or the application of any exemptions will lie exclusively with the CCG.

### 3.11 Personal Information

The CCG takes its duties and responsibilities for confidentiality and security of personal information very seriously and will generally remove or redact personal information from documents or records provided in response to an information access request unless the individual concerned has consented to the disclosure; the individual concerned is a staff member in a senior position; the personal information is already in the public domain; it is reasonable in all the circumstances to disclose the personal information.

### 3.12 Providing Advice and Assistance

The CCG does not expect the public to have a full understanding of all the information that it does or does not hold, and appreciates that some requestors may have difficulty framing their information access request in a way that enables it to respond.

The CCG will offer advice and assistance to requestors where there is any confusion about the nature of a request; when it is too unspecific so it is not clear as to what information is being sought; or the request is too broad or complex.

Although requestors do not need to state the reason for their information access request (except with AHRA), there will be occasions where knowing this can facilitate providing advice and assistance. The CCG will ask for reasons in a manner that clearly explains why it is asking but making it clear that the requestor is not obliged to answer.

The CCG will also provide advice and assistance to requestors who have difficulty making a request in writing due, for example, to communication issues or disability.

There may be occasions where individuals are unhappy with the way that the CCG responds to information access requests, either because they expected to receive more information or they disagree with the application of exemptions. Any complaints received will be handled in line with the CCG's complaints procedure.

### 3.12.1 Freedom of Information Act 2000 (FOIA)

Requestors can ask for an internal review within a reasonable time of receiving a response in line with the section 45 code of practice. This will be undertaken by someone not involved in handling the original request and the CCG will advise the requestor of the outcome as promptly as possible, normally within 20 working days but no later than 40 working days.

Regardless of whether the internal review upholds or overturns the original decision, in whole or in part, the CCG will advise the requestor of his/her right of appeal to the Information Commissioner.

### 3.12.2 Environmental Regulations 2004 (EIR)

Requestors have a legal right to make representations for review within 40 working days of the CCG's response. This will be undertaken by someone not involved in handling the original request and the CCG will advise the requestor of the outcome promptly but no later than 40 working days after receipt.

Regardless of whether the review upholds or overturns the original decision, in whole or in part, the CCG will advise the requestor of his/her right of appeal to the Information Commissioner.

### 3.12.3 Data Protection Act 2018 (DPA)

Although there are specific rights within DPA to require organisations to rectify incorrect personal information or to stop processing that information, there is no requirement for the CCG to have an internal review process for subject access requests. The requestor can appeal to the Information Commissioner for an assessment of whether the CCG has complied with legal requirements.

However the CCG will undertake an internal review following any complaint in line with its agreed complaints procedures and advise the requestor of the outcome as soon as possible, normally within 30 calendar days, including advising of the right to complain to the Information Commissioner.

**NB:** These timescales are likely to change under the GDPR and UK Data Protection Bill as determined by the Information Commissioner.

#### 3.12.4 Access to Health Records Act 1990 (AHRA)

The CCG will process complaints about information disclosed or withheld under AHRA in line with its agreed complaints procedure as with information disclosed or withheld under DPA. Requestors who remain dissatisfied will be advised to contact the Parliamentary and Health Service Ombudsman.

#### 3.13 Charging for Information

The CCG will only charge for providing copies of information in accordance with the relevant fees regulations and in line with its own schedule of charges current at the time of receipt of the information access request. In general charges will not apply to information provided electronically, but will apply to paper copies or provided on permanent storage media. Under the DPA 2018 Subject Access Requests and subjects rights Requests cannot be charged for unless they are considered manifestly unfounded or excessive.

The CCG may choose, at its discretion and without obligation, to waive all or part of any charge due in any particular case.

##### 3.13.1 Freedom of Information Act 2000 (FOIA)

The CCG will endeavour to charge the cost of printing, copying, postage and packaging in line with the current schedule of charges.

##### 3.13.2 Environmental Information Regulations 2004 (EIR)

The CCG will not charge for inspection of information by appointment but will normally charge the cost of printing, copying, postage and packaging in line with the current schedule of charges.

##### 3.13.3 Data Protection Act 2018 (DPA)

Subject access requests and Subject rights requests must be provided free of charge unless the request is manifestly unreasonable or excessive, whereby a reasonable fee may be charged based on administrative costs.

##### 3.13.4 Access to Health Records Act 1990 (AHRA)

The CCG may charge up to £10 to view the health record of a deceased patient. Copies of all or part of the record will be charged in line with the current schedule of charges.

#### 3.14 Re-use of Information

3.14.1 In general information provided by the CCG can only be re-used in line with normal copyright requirements or, in the case of AHRA, only for the purpose for which it was provided. Individuals can re-use their own personal information for any purpose they see fit.

3.14.2 The CCG will consider requests for wider use or for use on a commercial basis on a case by case basis in line with the rRe-use of Public Sector Information Regulations 2005. Requests for re-use must be made in writing, state the name of the requestor with an address for correspondence, specify the document or information requested and state the purpose for which re-use is requested. The consent of the data subject must always be gathered if it is intended to use their data in a manner other than that expected by the data subject or explained within the CCG's fair processing notice.

3.14.3 The CCG will respond within 20 working days making the requested document available to the requestor for re-use and advising of any applicable charges applicable for re-use. The requestor will also be advised of any conditions on which re-use will be permitted or if the request is refused, an explanation as to why.

3.14.4 The requestor will also be advised of the CCG's internal review process for complaints. Regardless of whether an internal review upholds or overturns the original decision, in whole or in part, the requestor will be advised of his/her right of appeal to the Office of Public Sector Information.

3.14.5 Information made available for re-use to the requestor can also be re-used by any other person or organisation as the CCG will not enter into exclusive use agreements.

#### 4. Duties and responsibilities

<b>Governing body</b>	The governing body (GB) for setting the strategic context in which organisational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents.
<b>Chief Officer</b>	The chief officer has overall responsibility for the strategic direction of information governance within the CCG, including ensuring that the CCG complies with all legal and statutory guidance requirements.
<b>Head of Corporate Affairs</b>	The head of corporate affairs has delegated responsibility from the chief officer for the strategic direction and operational delivery of the information governance function, including ensuring that all process documents comply with all legal, statutory and good practice guidance requirements.
<b>The Information Governance Team (NECS)</b>	The Information Governance team, will: <ul style="list-style-type: none"> <li>• undertake operational delivery of the information governance function on behalf of the CCG as specified in the service line agreement</li> <li>• prepare and collate evidence to support the CCG's self-assessment of the annual information governance toolkit</li> <li>• develop and implement operational processes and procedures for the information governance function</li> <li>• Provide information governance training for all staff to ensure they are aware of their responsibilities with regard to information security and confidentiality</li> <li>• Provide support and advice to staff in relation to information governance matters as required</li> <li>• Assist in the investigation of any incidents and development of action plans that occur as a result of failure to comply with this policy</li> <li>• Manage the Freedom of Information Act requests process on behalf of the CCG, receiving, assessing and subsequently disclosing information as appropriate.</li> </ul>

<p><b>Caldicott Guardian</b></p>	<p>The Caldicott Guardian is responsible for:</p> <ul style="list-style-type: none"> <li>• Representing and championing confidentiality requirements and issues and, where appropriate, at a range of levels within the CCG’s overall governance framework</li> <li>• Supporting work to facilitate and enable information sharing, advising on options for lawful and ethical processing of information as required.</li> </ul> <p>With support from the Head of Corporate Affairs and NECS Information Governance team, the Caldicott Guardian will:</p> <ul style="list-style-type: none"> <li>• Ensure the data protection work programme is successfully co-ordinated and implemented</li> <li>• Ensure the CCG complies 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</li> <li>• Complete the Confidentiality and Data Protection Assurance component of the Information Governance Toolkit, contributing to the annual assessment</li> <li>• Provide routine reports on Confidentiality and Data Protection issues.</li> </ul>
<p><b>Information Asset Owners (IAOs)</b></p>	<p>IAOs, with the assistance of information asset administrators (IAAs) where necessary will;</p> <ul style="list-style-type: none"> <li>• Ensure that information systems are used within the terms of the CCG’s Notification with the Information Commissioner and the requirements of the Data Protection Act and relevant Code of Practice (N.B. the requirement to notify is not in the GDPR and UK Data Protection Bill.</li> <li>• Undertake a privacy impact assessment when commencing a new project which involves personal information</li> <li>• Restrict the use of systems where appropriate to those authorised users who need access for organisational or other authorised work</li> <li>• Restrict the access to particular sets of personal data to those authorised users who need access for organisational or other authorised work</li> <li>• Maintain appropriate security measures for systems and any personal data held to avoid loss of the personal data or unauthorised disclosure of the personal data. Ensure that all copies of personal data output or obtained from systems, whether recorded on paper, by electronic means or any other form, are securely destroyed or erased when they are no longer required for organisational purposes.</li> <li>• Ensure that personal data held in systems are as accurate as possible, kept up-to-date and the team/department has an effective policy for erasing or deleting and removing personal data as soon as they are no longer required for organisational purposes.</li> <li>• Ensure that all authorised users of systems containing personal data have been properly trained and advised of the CCG’s requirements in respect of data protection.</li> <li>• Ensure that personal data is not removed from CCG premises except where specifically required for the execution of the legitimate functions of the CCG and with the express permission of the employee’s line manager. Advice should be sought from the Caldicott Guardian or Head of Corporate Affairs</li> <li>• Ensure that the Head of Corporate Affairs and NECS Information Governance team are advised as soon as possible of any incidents or complaints that need to be recorded.</li> </ul>

<b>Data Protection Officer (DPO)</b>	To providing expert advice and the promotion of data protection compliance and best practice in setting and maintaining standards and procedures across the CCG.
<b>All Staff</b>	<p>All staff, including temporary and agency staff and NECS staff working on behalf of the CCG, are responsible for:</p> <ul style="list-style-type: none"> <li>• Complying with all policies, procedures and expected standards of behaviour within the CCG</li> <li>• Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken</li> <li>• Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities</li> <li>• Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising their line manager accordingly.</li> <li>• Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager</li> <li>• Attending training / awareness sessions when provided.</li> </ul>

## 5. Implementation

- 5.1 This policy will be available to all staff for use in relation to the specific function of the policy.
- 5.2 All directors and managers are responsible for ensuring that relevant staff within their own directorates and departments have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

## 6. Training Implications

- 6.1 The sponsoring manager will ensure that the necessary training or education needs and methods required to implement this policy are identified and resourced or built into the delivery planning process. This may include identification of external training providers or development of an internal training process.

## 7. Related Documents

### 7.1 Legislation and statutory requirements

- Cabinet Office (2018) *Data Protection Act 2018* London: HMSO
- Cabinet Office (2005) *Freedom of Information Act 1998* London: HMSO
- Cabinet Office (1998) *Access to Health Records Act 1998* London: HMSO
- Cabinet Office (1998) *Environmental Information Regulations 2004* London: HMSO
- Cabinet Office. (1998) *Human Rights Act 1998*. London: HMSO
- General Data Protection Regulation (2016)

## **8. Monitoring, review and archiving**

### **8.1 Monitoring**

The Executive Committee will agree a method for monitoring the dissemination and implementation of this policy. Monitoring information will be recorded in the policy database.

### **8.2 Review**

8.2.1 The Executive Committee will ensure that this policy document is reviewed in accordance with the timescale specified at the time of approval. No policy or procedure will remain operational for a period exceeding three years without a review taking place.

8.2.2 Staff who become aware of any change which may affect a policy should advise their line manager as soon as possible who should inform the Head of Corporate Affairs. The Head of Corporate Affairs will then consider the need to review the policy or procedure outside of the agreed timescale for revision.

8.2.3 For ease of reference for reviewers or approval bodies, changes should be noted in the 'document history' table on the front page of this document.

### **8.3 Archiving**

The Head of Corporate Affairs will ensure that archived copies of superseded policy documents are retained in accordance with the DH Records Management Code of Practice for Health and Social Care 2016.

## 9. Equality analysis



An Equality Impact Assessment (EIA) is a process of analysing a new or existing service, policy or process. The aim is to identify what is the (likely) effect of implementation for different groups within the community (including patients, public and staff).

We need to:

- Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Equality Act 2010
- Advance equality of opportunity between people who share a protected characteristic and those who do not
- Foster good relations between people who share a protected characteristic and those who do not

This is the law. In simple terms it means thinking about how some people might be excluded from what we are offering.

The way in which we organise things, or the assumptions we make, may mean that they cannot join in or if they do, it will not really work for them.

It's good practice to think of all reasons why people may be excluded, not just the ones covered by the law. Think about people who may be suffering from socio-economic deprivation or the challenges facing carers for example.

This will not only ensure legal compliance, but also help to ensure that services best support the healthcare needs of the local population.

Think of it as simply providing great customer service to everyone.

As a manager or someone who is involved in a service, policy, or process development, you are required to complete an Equality Impact Assessment using this toolkit.

<b>Policy</b>	A written statement of intent describing the broad approach or course of action the Trust is taking with a particular service or issue.
<b>Service</b>	A system or organisation that provides for a public need.
<b>Process</b>	Any of a group of related actions contributing to a larger action.



**STEP 1 - EVIDENCE GATHERING**

<b>Name of person completing EIA:</b>	Senior Governance Officer, NECS
<b>Title of service/policy/process:</b>	Information Access Policy
Existing: <input checked="" type="checkbox"/> New/proposed: <input type="checkbox"/> Changed: <input type="checkbox"/>	
<b>What are the intended outcomes of this policy/service/process? Include outline of objectives and aims</b>	
This policy sets out the policy for access to information and the framework for responding to requests under statutory regimes including; Data Protection Act 1998; General Data Protection Regulation; Freedom of Information Act 2000; Access to Health Records Act 1990; Environmental Information Regulations 2004. The policy compliments other Information Governance policies.	
<b>Who will be affected by this policy/service/process? (please tick)</b>	
<input checked="" type="checkbox"/> Staff members <input type="checkbox"/> Other	
If other please state:	
<b>What is your source of feedback/existing evidence? (please tick)</b>	
<input type="checkbox"/> National Reports <input type="checkbox"/> Staff Profiles <input type="checkbox"/> Staff Surveys <input type="checkbox"/> Complaints/Incidents <input type="checkbox"/> Focus Groups <input checked="" type="checkbox"/> Previous EIAs <input type="checkbox"/> Other	
If other please state:	

Evidence	What does it tell me? (about the existing policy/process? Is there anything suggest there may be challenges when designing something new?)
National Reports	N/A
Staff Profiles	N/A
Staff Surveys	N/A
Complaints and Incidents	N/A
Staff focus groups	N/A
Previous EIA's	N/A
Other evidence (please describe)	N/A



**STEP 2 - IMPACT ASSESSMENT**

**What impact will the new policy/system/process have on the following staff characteristics: (Please refer to the 'EIA Impact Questions to Ask' document for reference)**

**Age** A person belonging to a particular age

No impact identified

**Disability** A person who has a physical or mental impairment, which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities

No impact identified

**Gender reassignment (including transgender)** Medical term for what transgender people often call gender-confirmation surgery; surgery to bring the primary and secondary sex characteristics of a transgender person's body into alignment with his or her internal self perception.

No impact identified

**Marriage and civil partnership** Marriage is defined as a union of a man and a woman (or, in some jurisdictions, two people of the same sex) as partners in a relationship. Same-sex couples can also have their relationships legally recognised as 'civil partnerships'. Civil partners must be treated the same as married couples on a wide range of legal matters

No impact identified

**Pregnancy and maternity** Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context.

No impact identified

**Race** It refers to a group of people defined by their race, colour, and nationality, ethnic or national origins, including travelling communities.

No impact identified

**Religion or belief** Religion is defined as a particular system of faith and worship but belief includes religious and philosophical beliefs including lack of belief (e.g. Atheism). Generally, a belief should affect your life choices or the way you live for it to be included in the definition.

No impact identified

**Sex/Gender** A man or a woman.

No impact identified

**Sexual orientation** Whether a person's sexual attraction is towards their own sex, the opposite sex or to both sexes

No impact identified

**Carers** A family member or paid [helper](#) who regularly looks after a child or a [sick](#), [elderly](#), or [disabled](#) person

No impact identified



**STEP 3 - ENGAGEMENT AND INVOLVEMENT**

**How have you engaged with staff in testing the policy or process proposals including the impact on protected characteristics?**

No engagement undertaken as this policy has received minor amendments only

**Please state how staff engagement will take place:**



**STEP 4 - METHODS OF COMMUNICATION**

**What methods of communication do you plan to use to inform staff of the policy?**

- Verbal – through focus groups and/or meetings     Verbal - Telephone  
 Written – Letter                       Written – Leaflets/guidance booklets  
 Email     Internet                       Other

**If other please state:**

**ACCESSIBLE INFORMATION STANDARD**

The Accessible Information Standard directs and defines a specific, consistent approach to identifying, recording, flagging, sharing and meeting the information and communication support needs of service users.

**Tick to confirm you have you considered an agreed process for:**

- √ **Sending out correspondence in alternative formats.**
- √ **Sending out correspondence in alternative languages.**
- √ **Producing / obtaining information in alternative formats.**
- √ **Arranging / booking professional communication support.**
- √ **Booking / arranging longer appointments for patients / service users with communication needs.**

**If any of the above have not been considered, please state the reason:**



**STEP 5 - SUMMARY OF POTENTIAL CHALLENGES**

Having considered the potential impact on the people accessing the service, policy or process please summarise the areas have been identified as needing action to avoid discrimination.

Potential Challenge	What problems/issues may this cause?
None identified.	



**STEP 6- ACTION PLAN**

Ref no.	Potential Challenge/ Negative Impact	Protected Group Impacted (Age, Race etc)	Action(s) required	Expected Outcome	Owner	Timescale/ Completion date
	None identified.					

Ref no.	Who have you consulted with for a solution? (users, other services, etc)	Person/ People to inform	How will you monitor and review whether the action is effective?



**SIGN OFF**

<b>Completed by:</b>	<b>Senior Governance Officer, NECS</b>
<b>Date:</b>	<b>June 2018</b>
<b>Presented to: (appropriate committee)</b>	<b>Executive Committee</b>
<b>Publication date:</b>	

## Summary of Key Legislation

### **Freedom of Information Act 2000 (FOIA)**

The FOIA applies to all public authorities, including health bodies like the CCG. It is domestic legislation resulting from public and political pressure for more openness and accountability in public life. The FOIA places a legal obligation on public authorities to pro-actively release corporate information like minutes of meetings, policies and procedures and annual reports through a 'guide to information' (previously a publication scheme).

In addition the public has the legal right to request access to information held by the CCG that is not routinely published. This includes information held in any format and regardless of whether originally produced by or for the CCG or received from other organisations or individuals. The FOIA also requires the Lord Chancellor to issue codes of practice and the Information Commissioner to promote the use of the codes and to measure the activities of public authorities against them (section 45 – procedural code for dealing with information access requests and section 46 – guidance code on records management).

### **Environmental Information Regulations 2004 (EIR)**

The EIR applies to all public authorities covered by the FOIA, but extends to include all organisations, private contractors or individuals carrying out 'public administration functions'.

The EIR enforces a European-wide directive allowing the public a right of access to a broad range of information about the environment including:

- The state of the elements of the environment such as air, water, soil, land
- Emissions and discharges, noise, energy, radiation, waste and other such substances;
- Measures and activities such as policies, plans, and agreements affecting or likely to affect the state of the elements of the environment
- Reports, cost-benefit and economic analyses used in these policies, plans and agreements
- The state of human health and safety, contamination of the food chain and cultural sites and built structures (to the extent they may be affected by the state of the elements of the environment).

Public authorities are also required to pro-actively publish environmental information and to progressively make that information available by electronic and easily accessible means. The EIR also allows the issue of a procedural code of practice by the Secretary of State on all aspects of dealing with information access requests. The Information Commissioner promotes the use of the current code and measures the activities of public authorities against it.

### **Data Protection Act 2018 (DPA)**

The DPA applies to all organisations, including public authorities and private companies, that process personal information about living individuals including their staff, customers,

patients and service users. Processing covers all actions taken, including collecting, storing, using, changing, sharing or destroying personal information. The DPA is domestic legislation that enforces a European-wide directive about protecting the privacy and confidentiality of personal information.

The DPA gives living individuals a range of rights related to their own personal information, including:

- The right to know who is processing their personal information, for what purpose and who else it may be shared with
- The right to prevent processing that is causing damage or distress
- The right to make a 'subject access request' to view their own personal information and/or to be provided with a copy of the information or record
- The right to have errors corrected
- The right to have their personal data held by an organisation erased
- The right to alter or prevent the processing of their personal data.

The legal rights under DPA are enhanced by the NHS Care Record Guarantee, which governs how patient information is used, what control patients have over their records and how they can be accessed. The Social Care Record Guarantee covers service user records.

Although the DPA only applies to protection of personal information for living individuals, it is NHS policy that the common law duty of confidence continues after death and this has been confirmed in guidance by the Information Commissioner. The CCG will generally restrict access to health records of deceased individuals to those with access rights under AHRA provisions.

The DPA was modernised data protection law in 2018 to meet the needs of an increasingly digital economy and society and provides a comprehensive legal framework for data protection in the UK, supplemented by the GDPR.

### **General Data Protection Regulations/UK Data Protection Bill**

The European Union General Data Protection Regulations (GDPR) which was adopted by the European Union in 2016 came into force in all EU Member States on 25 May 2018. The Data Protection Act 2018 incorporates and supplements the GDPR to create UK data protection legislation which is valid both pre and post Brexit. The new law aims to protect privacy, strengthen rights and empower individuals to have more control over their personal data by providing easier access. Individuals will generally have more control over their digital footprint, their personal data, how it is used and passed on by companies.

### **Access to Health Records Act 1990 (AHRA)**

The AHRA applies only to organisations that hold patient health records, including NHS bodies, private health providers and GP practices. It is domestic legislation allowing certain individuals to access the health records of deceased patients for specified purposes only. All other aspects of the AHRA no longer apply, as access to health records for living individuals is now included in the DPA.