NHS
North East and North Cumbria

Corporate	ICBP021 Information Access Policy

Version Number	Date Issued	Review Date
V1	July 2022	October 2022

Prepared By:	Senior Governance Manager, NECS
Consultation Process:	Integrated Governance Workstream
Formally Approved:	July 2022
Approved By:	Executive Committee

EQUALITY IMPACT ASSESSMENT

Date	Issues
December 2021	None

POLICY VALIDITY STATEMENT

Policy users should ensure that they are consulting the currently valid version of the documentation. The policy will remain valid, including during its period of review. However, the policy must be reviewed at least once in every 3-year period.

ACCESSIBLE INFORMATION STANDARDS

If you require this document in an alternative format, such as easy read, large text, braille or an alternative language please contact NECSU.Comms@nhs.net

Version Control

Version	Release Date	Author	Update comments
1.0	July 2022	Senior Governance Manager, NECS	First Issue

Approval

Role	Name	Date
Approver	Executive Committee	July 2022

Contents

1. Introduction

The ICB 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 ICB 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 ICB 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 ICB's statutory obligations. This policy will be available on the internet. in line with the Publication Scheme.

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 ICB 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 ICB 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 ICB complies with its statutory obligations.

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, and the ICB is committed to this policy and its implementation.

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

This document sets out the Information Access Request Policy for the ICB 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 (GDPR);
- 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 & monitoring requests for information.

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

2. Definitions

The following terms are used in this document:

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, National Insurance Number, etc. It also includes information which, when presented in combination, may identify an individual e.g. postcode, date of birth etc. Pseudonymised information is classed as personal because it can be re-identified.

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.” Social care record is not defined.

2.4 **Corporate Information:** is held in corporate records which relate to the business of the ICB 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 Request:** 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 ICB. This includes family members of an individual, legal representatives, contractors working for and partner organisations working with the ICB.

2.9 **Re-use of Information:** means the use by any person or organisation of a document, record or information held by the ICB for a purpose other than the initial purpose for 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.

Note: The GDPR refers to a "supervisory authority" in EU member states – in the UK the Information Commissioner is the supervisory authority.

2.12 **Attorney:** 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 is 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) adaptation 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, "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. The DPA 2018 replicates this.

2.17 **Data Subject:** A living individual who is the subject of personal data / information.
The DPA 2018 defines a 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.

In GDPR 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.

Note: GDPR defines 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.”

2.19 **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.

2.20 **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.

2.21 **Applicant:** Individual(s) or Trust requesting access to information under the FOI Act.

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

2.23 **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.

2.24 **Fees 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.

2.25 **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 to be provided a copy of the information unless an exemption applies.

2.26 **Lord Chancellor's Department:** Government department responsible for the efficient administration of justice in England and Wales.

2.27 **Publication Scheme:** Scheme specifying the classes of information which a public authority publishes or intends to publish.

3. Information Access Requests

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

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

Although information access requests under the FOIA must be made in writing, the ICB appreciates this may cause difficulties for some requestors due to, for example, communication issues or disability, and 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 2000 (FOIA)

3.1.1 Published Information

3.1.1.1 Under FOIA all public authorities are obliged to adopt and maintain an approved Publication Scheme.

3.1.1.2 The ICB 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.

3.1.1.3 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.

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

3.1.2 Unpublished Information

3.1.2.1 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 information access request or to prove their identity. Neither are they required to state why they require the information or the purpose of their request, although this can assist in identifying the information requested.

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

3.1.2.3 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 need not be made in writing; the information access request could 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 to clarify it and the ICB will offer advice and assistance to them to do so. If the request is still too general, the ICB 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

3.3.1.1 Subject access requests for personal information under the DPA must be made by the living individual concerned or his/her representative. The request must include evidence of identity, enough information to locate the relevant files or records and, in the case of a representative, evidence of authority to act.

3.3.1.2 The ICB is most likely to receive information access requests from patients, service users, staff and contractors and these can only be accepted from: the individual concerned; his/her authorised representative; an adult with parental responsibilities for children under the age of 13 or where a child is not competent to make their own decisions; an attorney with authority to manage the affairs of an individual with or without the mental capacity to manage their own affairs; any person appointed by the Court of Protection to act on behalf of an individual without the mental capacity to manage their own affairs.

3.3.1.3 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

3.3.2.1 The ICB will not generally disclose personal information about living individuals, in compliance with the requirements of DPA and the common law duty of confidence.

3.3.2.2 There will be occasions, however, when the ICB 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.

3.3.2.3 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 where required by a Coroner in relation to an unexpected or suspicious death.

3.3.2.4 Other investigatory bodies may also request information, including the Police and Revenue and Customs (HMRC). They must provide the ICB with a written explanation of why the information is required and the likely effect on investigation or prosecution if it is not provided. The ICB 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.

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

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

3.3.2.6 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 ICB 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 ICB 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

The ICB will respond to all information access requests in line with legislative requirements for timeliness and completeness and in accordance with its own procedures current at the time of receipt of the request.

The ICB's default position is to release the information requested unless there is a very good or legal reason not to do so. Occasionally the ICB will respond by issuing a refusal notice as detailed in Section 3.6 below rather than by providing some or all of the information requested.

The ICB will provide the information requested in the format specified by the requestor whenever reasonably practicable. If it is not possible to provide information in the preferred format, the ICB will explain the reason why. Where appropriate the ICB 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 ICB will explain the appeals and complaints process in its responses.

3.5.1 <u>Freedom of Information Act 2000 (FOIA)</u>

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

3.5.1.2 The only exceptions will be where the ICB is considering the public interest test regarding the applicability of one of the 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, in which case the ICB will seek clarification from the requestor before responding; where charges are applicable, the ICB will issue a fees notice to the requestor.

3.5.1.3 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)

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

3.5.2.2 The only exceptions will be where the request is particularly complex or involves providing large amounts of information. Within 20 working days, the ICB will either inform the requestor that 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.

3.5.2.3 If charges are applicable, the ICB will issue a fees notice 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)

3.5.3.1 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, the individual must be informed within one month of the receipt of the request and given an explanation as to why the extension is necessary.

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

3.5.4 Access to Health Records Act 1990 (AHRA)

3.5.4.1 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. There is no fee.

3.5.4.2 The ICB 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.

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

Where only part of a document, record or other information is exempt the ICB will remove or redact the exempt information only and the remainder of the requested information will be provided.

The ICB 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)

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

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

3.6.1.3 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. The ICB will disclose qualified information if, on balance, the public interest in disclosing exempted information is equal to or greater than the public interest in withholding.

3.6.1.4 The ICB 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.

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

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

3.6.2 Environmental Information Regulations 2004 (EIR)

3.6.2.1 The ICB may withhold information 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.

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

3.6.2.3 The ICB may refuse a request if it is manifestly unreasonable or too general, but will provide advice and assistance to make the request more manageable. Requests relating to unfinished documents or data can also be refused, although the ICB will inform the requestor when the information is expected to become available.

3.6.2.4 If the ICB 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 2018 (DPA)

3.6.3.1 The ICB may withhold some or all of the personal information of the requestor 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 ICB's ability to bring or defend legal proceedings; disclosure would be likely to affect the prevention or detection of crime.

3.6.3.2 The ICB 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.

3.6.3.3 If the ICB withholds information based on an exemption it will issue a refusal notice explaining: what exemption it has applied and why; the internal review process; the requestor's right to complain to the Information Commissioner.

3.6.4 Access to Health Records Act 1990 (AHRA)

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

3.6.4.2 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.

3.6.4.3 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.

3.6.4.4 If the ICB withholds information based on an exemption it will issue a refusal notice explaining: what exemption it has applied and why; the internal review process; the requestor's right to complain to the Parliamentary & Health Service Ombudsman.

3.7 Transferring Requests for Information

3.7.1 If the ICB 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; providing the requestor with contact details for that authority and suggesting s/he reapplies to them; if the requester indicates that they do not object to the transfer of the request to the other public authority, The ICB may transfer the request directly, notifying the requestor if this is to be done.

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

3.7.4 The ICB 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 Subject 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 ICB 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 ICB 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 ICB 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 ICB 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 ICB 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 ICB 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 ICB will, however, 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 The ICB will consult before disclosure of any information obtained from other organisation or during joint working, to take account of the potential effect that disclosure may have on the functions of third party partner organisations.

3.10.2 The final decision about disclosure and/or the application of any exemptions will, however, lie exclusively with the ICB.

3.11 Personal Information

The ICB 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 information is about staff which is considered to be subject to disclosure; 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 ICB 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 ICB will offer advice and assistance to requestors where there is any confusion about the nature of a request, if it is so unspecific as to not be clear what information is being sought or the request is too broad or complex for response.

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 ICB will ask about the reasons in a manner that clearly explains why it is asking, and that the requestor is not obliged to answer.

The ICB will provide advice and assistance to requestors who have difficulty making an information access request in writing due, for example, to communication issues or disability.

There may be occasions where individuals are unhappy with the way that the ICB responds to information access requests, either because they expected to receive more information or they disagree with the application of exemptions.

Complaints will be handled taking account of legislative requirements and relevant codes of practice, although the ICB will normally attempt to resolve matters informally in the first instance.

3.12.1 Freedom of Information Act 2000 (FOIA)

3.12.1.1 Requestors can ask for an internal review within a reasonable time of receiving the ICB's response, in line with section 45 of the code of practice.

3.12.1.2 This will be undertaken by someone not involved in handling the original request. The ICB will advise the outcome as promptly as possible, normally within 20 working days and no later than 40 working days.

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

3.12.2 Environmental Information Regulations 2004 (EIR)

3.12.2.1 Requestors have a legal right to make representations for review within 40 working days of the ICB's response.

3.12.2.2 This will be undertaken by someone not involved in handling the original request. The ICB will advise the outcome promptly and no later than 40 working days after receipt.

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

3.12.3 Data Protection Act 2018 (DPA)

3.12.3.1 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 ICB to have an internal review process for subject access requests. The requestor can appeal to the Information Commissioner for an assessment of whether the ICB has complied with legal requirements.

3.12.3.2 The ICB will, however, undertake an internal review voluntarily following any complaint and will advise the outcome as promptly as possible, normally within 30 calendar days, including advising the requestor of the right to complain to the Information Commissioner.

3.12.4 Access to Health Records Act 1990 (AHRA)

The ICB will process complaints about information disclosed or withheld under AHRA as with information disclosed or withheld under DPA, with the exception that requestors who remain dissatisfied will be advised to contact the Parliamentary and Health Service Ombudsman.

3.13 Charging for Information

The ICB 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. There is no fee for AHRA requests.

The ICB 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 ICB 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 ICB 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)

3.13.3.1 Subject Access Requests and Subjects 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)

3.13.4.1 The Data Protection Act 2018 has amended the Access to Health Records Act 1990, which now states access to the records of deceased patients and any copies must be provided free of charge.

3.14 Re-use of Information

3.14.1 In general, information provided by the ICB 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, but individuals can re-use their own personal information for any purpose they see fit.

3.14.2 The ICB will consider requests for wider use or for use on a commercial basis on a case by case basis in line with the Re-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; 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 ICBs Fair Processing Notice.

3.14.3 The ICB will respond within 20 working days, making the requested document available to the requestor for re-use; advising of the charges applicable for re-use, if any; advising the requestor of any conditions on which re-use will be permitted, if any; or refusing the request and explaining why.

3.14.4 The ICB's response will advise the requestor of the internal review process for complaints. Regardless of whether an internal review upholds or overturns the original decision, in whole or in part, the ICB will advise the requestor 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 ICB will not enter into 'exclusive use' agreements.

4. Implementation

4.1 This policy will be available to all staff for use in relation to the specific function of the policy.

4.2 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.

5. Training Implications

It has been determined that there are no specific training requirements associated with this policy. However mandatory Data Security Awareness training must be completed by all staff annually

6. Documentation

6.1 Other related policy documents.

- Information Governance and Information Risk Policy
- Subject Access Request and Data Subject Rights Request Standard Operating Procedure

6.2 Legislation and statutory requirements

- Cabinet Office (2018) *Data Protection Act 2018* London: HMSO
- Cabinet Office (2005) *Freedom of Information Act 2000* London: HMSO
- Cabinet Office (1998) *Access to Health Records Act 1990 London*: HMSO
- Cabinet Office (1998) *Environmental Information Regulations 2004* London: HMSO
- Cabinet Office. (1998) *Human Rights Act 1998*. London: HMSO
- General Data Protection Regulations (2016)

6.3 Best practice recommendations

- ICO – Guide to Data Protection https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
- ICO – Guide to Freedom of Information https://ico.org.uk/for-organisations/guide-to-freedom-of-information/
- ICO – Guide to the Environmental Information Regulations https://ico.org.uk/for-organisations/guide-to-the-environmental-information-regulations/

7. Monitoring, Review and Archiving

7.1 Monitoring

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

7.2 Review

7.2.1 The ICB Board 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.

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

7.2.3 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.

NB: If the review consists of a change to an appendix or procedure document, approval may be given by the Executive director and a revised document may be issued. Review to the main body of the policy must always follow the original approval process.

7.3 Archiving

The ICB Board will ensure that archived copies of superseded policy documents are retained in accordance with the NHS Records Management Code of Practice 2021.

Schedule of Duties and Responsibilities

Through day to day work, employees are in the best position to recognise any specific fraud risks within their own areas of responsibility. They also have a duty to ensure that those risks, however large or small, are identified and eliminated. Where it is believed fraud, bribery or corruption could occur, or has occurred, this should be reported to the CFS or the chief finance officer immediately.

ICB Board	The ICB Board has responsibility 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.
Chief Executive	The Chief Executive has overall responsibility for the strategic direction and operational management, including ensuring that ICB process documents comply with all legal, statutory and good practice guidance requirements
Senior Governance Manager	The Senior Governance Manager as author will ensure this policy is kept up to date in line with legislation and best practice.
The Information Governance Team	The Information Governance team will; • Make available information governance training for all staff to ensure they are aware of their responsibilities with regard to information security and confidentiality. • Monitor that staff are aware of these responsibilities. • Assist in the investigation of any incidents and development of action plans that occur as a result of failure to comply with this policy.

Caldicott Guardian	The Caldicott Guardian is responsible for; • Representing and championing confidentiality requirements and issues and, where appropriate, at a range of levels within the ICB's overall governance framework. • Supporting work to facilitate and enable information sharing, advising on options for lawful and ethical processing of information as required. With support from the Information Governance team, the Caldicott Guardian will: • Ensure the data protection work programme is successfully co-ordinated and implemented. • Ensure the ICB 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. • Complete the Confidentiality and Data Protection Assurance component of the Data Security and Protection Toolkit, contributing to the annual assessment. • Provide routine reports on Confidentiality and Data Protection issues.
Data Protection Officer	To take the lead in providing expert advice and the promotion of data protection compliance and best practice in setting and maintaining standards and procedures across the ICB.
Freedom of Information Officer	To be responsible for receiving, assessing and subsequently disclosing information in response to requests made to the ICB under the Freedom of Information Act 2000 (FoIA).

Information Asset Owners (IAOs)	IAOs, with the assistance of Information Asset Administrators (IAAs) where necessary will; • Ensure that the system is used within the terms of the ICB's Notification with the Information Commissioner and the requirements of both data protection legislation and the relevant Code of Practice, paying particular attention to the data protection principles as specified in the Act. • When developing a new process, or changing an existing process, complete an information governance checklist. This will help to ensure any issues are highlighted and dealt with at an early stage. • Participate in a Privacy Impact Assessment when commencing a new project which involves personal information. • Restrict the use of the system where appropriate to those authorised users who need access to it for organisational or other authorised work. • Restrict the access to particular sets of personal data available from the system to those authorised users who need access to them for organisational or other authorised work. • Maintain appropriate security measures for the system and any personal data held within it 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 the system, whether recorded on paper or by electronic means or any other form, are securely destroyed or erased when they are no longer required for organisational purposes. • Ensure that personal data held in the system are as accurate as possible and kept up-to-date where relevant and that the department has an effective policy for erasing or deleting and removing personal data as soon as they are no longer required for organisational purposes. • Ensure that all authorised users of the system containing personal data have been properly trained and advised of the ICB's requirements in respect of data protection. • Ensure that personal data is not removed from the ICB's premises except where specifically required for the execution of the legitimate functions of the ICB, and with the express permission of the employee's Line Manager. Advice should be sought from the Caldicott Guardian or Information Governance team. • Ensure that the Information Governance team is advised as soon as possible of any incidents or complaints that need to be recorded in Incident reporting system.

Commissioning Support Staff.	Whilst working on behalf of the ICB NECS staff will be expected to comply with all policies, procedures and expected standards of behaviour within the ICB, however they will continue to be governed by all policies and procedures of their employing organisation.
All Staff	All staff, including temporary and agency staff, are responsible for: • Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken. • Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities. • 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. • Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager. • Attending training / awareness sessions when provided.

Appendix A – Equality Impact Assessment

Equality Impact Assessment
Initial Screening Assessment (STEP 1)

As a public body organisation we need to ensure that all our current and proposed strategies, policies, services and functions, have given proper consideration to equality, diversity and inclusion, do not aid barriers to access or generate discrimination against any protected groups under the Equality Act 2010 (Age, Disability, Gender Reassignment, Pregnancy and Maternity, Race, Religion/Belief, Sex, Sexual Orientation, Marriage and Civil Partnership).

This screening determines relevance for all new and revised strategies, policies, projects, service reviews and functions.

Completed at the earliest opportunity it will help to determine:

- The relevance of proposals and decisions to equality, diversity, cohesion and integration.
- Whether or not equality and diversity is being/has already been considered for due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED).
- Whether or not it is necessary to carry out a full Equality Impact Assessment.

Name(s) and role(s) of person completing this assessment:

Name: Liane Cotterill
Job Title: Senior Governance Manager
Organisation: North of England Commissioning Support Unit

Title of the service/project or policy: Information Access Policy

Is this a;
Strategy / Policy ☒ **Service Review** ☐ **Project** ☐
Other Click here to enter text.

What are the aim(s) and objectives of the service, project or policy:
This policy sets out the Information Access Request Policy for the ICB 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 (GDPR);
- Access to Health Records Act 1990 (AHRA).

Who will the project/service /policy / decision impact?
(Consider the actual and potential impact)

- **Staff ☒**
- **Service User / Patients ☐**
- **Other Public Sector Organisations☐**
- **Voluntary / Community groups / Trade Unions ☐**
- **Others, please specify** Click here to enter text.

Questions	Yes	No
Could there be an existing or potential negative impact on any of the protected characteristic groups?	☐	☒
Has there been or likely to be any staff/patient/public concerns?	☐	☒
Could this piece of work affect how our services, commissioning or procurement activities are organised, provided, located and by whom?	☐	☒
Could this piece of work affect the workforce or employment practices?	☐	☒
Does the piece of work involve or have a negative impact on: • Eliminating unlawful discrimination, victimisation and harassment • Advancing quality of opportunity • Fostering good relations between protected and non-protected groups in either the workforce or community	☐	☒

If you have answered no to the above and conclude that there will not be a detrimental impact on any equality group caused by the proposed policy/project/service change, please state how you have reached that conclusion below:

Policy is based on legislation requirements, no negative impact identified.

If you have answered yes to any of the above, please now complete the 'STEP 2 Equality Impact Assessment' document

Accessible Information Standard	Yes	No
Please acknowledge you have considered the requirements of the Accessible Information Standard when communicating with staff and patients. https://www.england.nhs.uk/wp-content/uploads/2017/10/accessible-info-standard-overview-2017-18.pdf	☒	☐
Please provide the following caveat at the start of any written documentation: **"If you require this document in an alternative format such as easy read, large text, braille or an alternative language please contact (ENTER CONTACT DETAILS HERE)"**		

If any of the above have not been implemented, please state the reason:
Click here to enter text.

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	**Job title**	**Date**
Executive Committee	Approver	July 2022

Publishing

This screening document will act as evidence that due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED) has been given.

If you are not completing 'STEP 2 - Equality Impact Assessment' this screening document will need to be approved and published alongside your documentation.

Please send a copy of this screening documentation to: NECSU.Equality@nhs.net for audit purposes.

Appendix B - Summary of Key Legislation

Freedom of Information Act 2000 (FOIA)

The FOIA applies to all public authorities, including health bodies like the ICB. 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 & procedures and annual reports through Publication Scheme.

In addition, the public has the legal right to request access to information held by the ICB that is not routinely published. This includes information held in any format and regardless of whether originally produced by or for the ICB or received from other organisations or individuals.

Codes of Practice: 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;
- 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 Europe 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.

Code of Practice: 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 Europe 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 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, and 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 can have over their records and how they can be accessed, and the Social Care Record Guarantee which 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 ICB will, therefore, generally restrict access to health records of deceased individuals to those with access rights under AHRA provisions.

The DPA was modernised by 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 Regulation/UK Data Protection Bill

The European Union **G**eneral **D**ata **P**rotection **R**egulations (**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 included in the DPA.