

# Individual Rights Policy



**Please complete the table below:**

To be added by corporate team once policy approved and before placing on website

<b>Policy ref no:</b>	34
<b>Responsible Executive Director:</b>	Shane Devlin, Chief Executive
<b>Author and Job Title:</b>	Lucy Powell, Corporate Support Officer
<b>Date Approved:</b>	1 July 2022 (as part of the Core Policies approval) 1 <sup>st</sup> February 2024
<b>Approved by:</b>	ICB Board
<b>Date of next review:</b>	February 2026 (Every two years)

**Policy Review Checklist**

	<b>Yes/ No/NA</b>	<b>Supporting information</b>
Has an Equality Impact Assessment Screening been completed?	Yes	See appendix 1
Has the review taken account of latest Guidance/Legislation?	Yes	The Policy is compliant with: the Data Protection Act 2018 and the UK General Data Protection Regulation 2018 (the Data Protection legislation)
Has legal advice been sought?	No	Specialist advice has been taken from Information Governance Advisors. Information Governance is represented on the Corporate Policy Review Group
Has HR been consulted?	Yes	HR have been made aware that staff have a right to request personal data held by the ICB. HR is represented on the Corporate Policy Review Group.
Have training issues been addressed?	Yes	Training is referenced in the policy. The ICB's Information Governance training includes Information Rights; this training is

	Yes/ No/NA	Supporting information
		mandatory and annual. Training on ICB specific procedures as set out in the appendix will be tailored to relevant staff groups and will be at least annual.
Are there other HR related issues that need to be considered?	Yes	Staff are able to make Subject Access Requests to request data HR hold. The HR team have developed a form for requests and this is available to staff on the Consult HR website. Staff have been informed of their rights through internal communications.
Has the policy been reviewed by Staff Partnership Forum?	No	The policy does not raise any HR issues and has not been reviewed by the SPF.
Are there financial issues and have they been addressed?	No	There are no financial issues.
What engagement has there been with patients/members of the public in preparing this policy?	N/A	This policy describes a statutory responsibility and there has been no engagement with patients/members of the public beyond that undertaken by government as part of the legislative process
Are there linked policies and procedures?	Yes	Associated policies and procedures are recorded in the policy
Has the lead Executive Director approved the policy?	Yes	Shane Devlin, Chief Executive
Which Committees have assured the policy?		Corporate Policy Review Group and Audit and Risk Committee. Both provided feedback which has been included.
Has an implementation plan been provided?	Yes	See Appendix 2

	<b>Yes/ No/NA</b>	<b>Supporting information</b>
How will the policy be shared with staff, patients and the public?		The policy will be published on the ICB website and intranet and will be featured in the internal news communication. Implementation will be monitored through Information Rights reports to the Audit and Risk Committee
Will an audit trail demonstrating receipt of policy by staff be required; how will this be done?	No	
Has a DPIA been considered in regards to this policy?	Yes	A DPIA has been developed and approved
Have Data Protection implications have been considered?	Yes	The Policy is compliant with the Data Protection Act 2018 and the UK General Data Protection Regulation 2018

## Table of Contents

<b>Table of Contents</b> .....	<b>5</b>
<b>1 Introduction</b> .....	<b>7</b>
1.1 BNSSG ICB Values.....	7
<b>2 Purpose and scope</b> .....	<b>7</b>
<b>3 Duties – legal framework for this policy</b> .....	<b>8</b>
<b>4 Responsibilities and Accountabilities</b> .....	<b>9</b>
<b>5 Definitions/explanations of terms used</b> .....	<b>10</b>
<b>6 Managing requests for Information</b> .....	<b>11</b>
6.1 Recognising an Individual Rights Request.....	12
6.2 Refusing a request .....	12
6.3 Time Limits for Compliance with Requests .....	13
6.4 Charging a Fee .....	14
6.5 Verifying Identity.....	14
6.6 Retrieving Information .....	14
6.7 Redaction of Third Party Data.....	14
6.8 Special Cases: Health Records.....	15
<b>7 Access to Health Records Act 1990</b> .....	<b>16</b>
<b>8 Requests for information made on behalf of an Individual</b> .....	<b>16</b>
<b>9 Training requirements</b> .....	<b>17</b>
<b>10 Equality Impact Assessment</b> .....	<b>17</b>
<b>11 Implementation and Monitoring Compliance and Effectiveness</b> .....	<b>17</b>
<b>12 Countering Fraud, Bribery and Corruption</b> .....	<b>17</b>
<b>13 References, acknowledgements and associated documents</b> .....	<b>17</b>
<b>14 Appendices</b> .....	<b>19</b>
14.1 Equality Impact Assessment.....	19
14.2 Implementation Plan .....	25
14.3 The Individual Rights in more detail.....	26
14.4 Right to Access (Subject Access Request) Procedure .....	30

14.5 Right to Access (Subject Access Request) Internal Review Procedure.....31  
14.6 Consent Procedures .....32

# Individual Rights Policy

## 1 Introduction

Bristol, North Somerset and South Gloucestershire Integrated Care Board (BNSSG ICB) is under a legal duty to comply with 'individual's rights' requests under the Data Protection Legislation, in relation to personal data that it holds. It is a legal requirement that all requests for personal data held by the ICB are handled in accordance with data protection legislation.

This policy and accompanying standard operating procedure (SOP) sets out the approach that the ICB will take in responding to these requests along with useful guidance and steps to follow when requests are received anywhere within the ICB.

### 1.1 BNSSG ICB Values

This policy supports the values by outlining the process through which a statutory obligation will be fulfilled therefore demonstrating "We do the right thing". This Policy outlines the expectation that staff will "Act with integrity" by complying with Data Protection legislation. The Policy also "Supports each other" by providing information to support staff in responding to requests.

## 2 Purpose and scope

The policy sets out the ICB's legal obligation to comply with the Data Protection legislation in providing access to personal data. The Policy is not designed to be a guide for ICB staff in complying with Data Protection legislation. Guidance for staff will be provided through training and procedural documentation. (Appendix 4).

This policy applies to all staff, regardless of whether they hold a corporate or clinical role and includes:

- Individuals on the ICB Board and Committees
- Employees including those seconded to BNSSG ICB
- Third parties acting on BNSSG ICB's behalf (including commissioning support and shared services)
- Agency, locum and other temporary staff engaged by BNSSG ICB
- Students, including those on work experience, trainees and apprentices.

It is the responsibility of all those individuals set out above to respond to and help process requests under the individual rights set out in data protection legislation as soon as it is received by the ICB. Requests must be sent to the Information Rights team who will process the request: [bnssg.foi@nhs.net](mailto:bnssg.foi@nhs.net)

Any personal data in relation to an individual, no matter what format, where or how it is stored by the ICB falls into the scope of information that can be requested by individuals (i.e. data subjects) under the 'Individuals Right's' contained within the Data Protection Legislation. Individuals have the right to request a copy of their personal data which is being processed by controllers. All requests must be reviewed, without delay to see if the request can and should be complied with.

Requests received by third parties in regard to access to a data subjects personal data should be handled using the process described within the Standard Operating Procedure. Information regarding consent documentation required to open a request and further considerations have been included in Appendix 6.

### **3 Duties – legal framework for this policy**

The UK GDPR, which was implemented through the DPA 2018, gives individuals the right of access to their personal data from any organisation which holds records on them. The right is commonly referred to as 'subject access'. The right of access is one of many rights implemented so individuals can understand how and why organisations are using their data.

An individual can make a rights request verbally or in writing and to be valid must be a request for their own personal data. An individual may ask a third party to make a request on their behalf and before processing the request, the ICB must be assured that the third party is acting on behalf of the individual.

The Information Commissioners Office (ICO) may take action against a controller or processor if they fail to comply with data protection legislation.

The ICB must provide individuals with information including (but not limited to):

- A description of the information
- The purposes the information is used for
- Our retention periods for that personal data
- The disclosures that are made or might be made

This is called 'Privacy Information' or 'Fair Processing Information'. The ICB Fair Processing Notice is available on the ICB website. This information must be regularly reviewed and where necessary updated. The ICB SIRO is responsible for approval to changes in the Privacy notice.



## 4 Responsibilities and Accountabilities

The Chief Executive has overall responsibility for the Information Rights Policy. The implementation and compliance with the policy is delegated to the Corporate Secretary. This responsibility includes:

- Setting out a process for dealing with Information Rights requests within the timescales stated by the legislation.
- Facilitating the provision of education and awareness for staff, ensuring that basic principles are part of the ICB's induction processes.
- Bi-Annual review of policy, process and code of practice (or more frequently if appropriate, with regard to changes in legislation or guidance from the Information Commissioner)

The Information Rights team are responsible for the delivery of the functions related to processing and responding to Information Rights requests. This responsibility includes:

- Acknowledging and logging requests
- Sending requests to the appropriate team for a response
- Reviewing all the data and undertaking redactions as required
- Logging all the redactions made
- Facilitating Executive Director approval processes and sending the final response to the requester
- Processing and managing the internal review process

All staff are responsible for:

- Creating and maintaining records which are accurate, appropriate and retrievable. This will include adherence to standards for referencing, titling, filing and authoring documents, both electronically and on paper. The Records Management Policy defines the expectations of staff and should be read in conjunction with the Information Rights policies.
- Ensuring that requests for information are passed in a timely manner to staff who process Information Rights requests.
- Ensuring that disclosures are not made outside of the defined process, so that inappropriate disclosures are avoided.

Staff responsibilities are set out in contracts of employment. A breach of these responsibilities could result in disciplinary action.

The NHS South, Central and West Commissioning Support Unit (SCW CSU) Information Governance Team is responsible for overseeing day to day information governance issues and raising awareness of information governance related to this policy within the ICB. Support and delivery of matters associated with IG will be provided by SCW CSU, and the ICB Information Governance Group chaired by the SIRO.

The ICB Data Protection Officer will provide advice and guidance in complex or disputed situations or decisions where required. The ICB Caldicott Guardian will provide advice and guidance in complex situations or decisions where the issue is clinical in nature. The ICB SIRO will approve changes to the Privacy Notice

Line Managers are responsible for ensuring that staff are aware of requirements associated with this policy including the need to pass information to the Information Rights team promptly, and prioritising work to support timely responses.

## 5 Definitions/explanations of terms used

<b>Controller</b>	A controller determines the purposes and means of processing personal data. Previously known as Data Controller but re-defined under the GDPR.
<b>Personal Data</b>	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
<b>Personal Confidential Data</b>	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal data about identified or identifiable individuals, which should be kept private or secret. The definition includes deceased as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'.
<b>Processor</b>	A processor is responsible for processing personal data on behalf of a controller.
<b>'Special Categories' of Personal Data</b>	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: <ul style="list-style-type: none"> <li>(a) The racial or ethnic origin of the data subject</li> <li>(b) Their political opinions</li> <li>(c) Their religious beliefs or other beliefs of a similar nature</li> </ul>

	<p>(d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998</p> <p>(e) Genetic data</p> <p>(f) Biometric data for the purpose of uniquely identifying a natural person</p> <p>(g) Their physical or mental health or condition</p> <p>(h) Their sexual life</p>
<b>Healthcare Professional</b>	ICO guidance allows for the disclosure of 3 <sup>rd</sup> party data of healthcare professionals (most likely names) where they have contributed to a health record for an individual. A healthcare professional is defined as: A person associated with either a speciality or discipline and who is qualified and allowed by regulatory bodies to provide a healthcare service to a patient.
<b>Healthcare Record</b>	A healthcare record is defined as a record which stores information about a person's health, care and wellbeing

## 6 Managing requests for Information

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under UK Data Protection legislation. These rights fall into two distinct categories. Firstly, where an individual wants to know what data the ICB is processing about them and why, and/or receive a copy of that data. Secondly where an individual wants the ICB to make changes to what or how the ICB is processing their personal data, or for the ICB to pass on their personal data to another party. In these requests, the individual is not requesting a copy of the data itself.

These rights include but are not limited to the following:

- The right to be informed
- The right of access
- The right of rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

An individual or their representative can exercise these rights to the ICB. These do not confer automatic agreement to the request but will be duly considered by the ICB. Acknowledgement and processing of requests will be undertaken by the Information Rights team. The rights are outlined in more detail in appendix 3.

It should be noted that there are exemptions to some of these rights and whilst the ICB must acknowledge the request, there may be legal grounds for not complying with it. Detailed guidance can be found within the Standard Operating Procedures (SOP).

### 6.1 Recognising an Individual Rights Request

A request can be made verbally or in writing and can be sent to anyone within the organisation. A request does not need to mention that the request is a 'right' or mention Data Protection legislation for the request to be valid. The request needs to be clearly described to be valid. If the ICB is unsure of the request, the requester will be contacted for further information. The ICB will contact the requester to ask for identification/authorisation if required. The types of identification/authorisation required are included in appendix 6. The ICB will keep a record of all requests received. This record will be updated and maintained by the Information Rights team.

The format that a request is received may differ from request to request. If an individual writes or speaks to the ICB and asks for access, changes or objections of any kind to the personal data the ICB is processing about them (whether perceived or actual) it should be considered and handled where appropriate as an Individual Rights request. Staff should contact the Information Rights Team who will process the request:

[bnssg.foi@nhs.net](mailto:bnssg.foi@nhs.net)

Members of the public who would like to exercise their individual rights under Data Protection legislation can submit their requests to [bnssg.foi@nhs.net](mailto:bnssg.foi@nhs.net)

Subject access requests can be made by:

- The individual themselves
- Individuals requesting access on behalf of a child for whom they have parental responsibility
- A representative nominated by the individual to act their behalf such as solicitors or a relative, where there is valid consent by the individual granting this authority
  - In certain situations a person granted an attorney or agent by the Court of Protection on behalf of an adult who is incapable of consent
  - Requests from public bodies and law enforcement agencies (Police, criminal court etc)

ICB staff can submit a request for access to their personal data verbally or in writing. A staff subject access request application form is available from HR for staff to use if they wish.

### 6.2 Refusing a request

The ICB is committed to comply with SARs. There are, however, occasions when a SAR may be refused or timelines to response to a SAR extended.

If the ICB considers that a request is 'manifestly unfounded' or excessive or repetitive in nature the ICB can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request

In either case the ICB will outline the reasons why, their right to complain to the ICO and their ability to seek to enforce a right through a judicial remedy.

The ICO defines 'manifestly unfounded' as:

- The individual has no intention to exercise their right of access. For example, makes a request but offers to withdraw the request in return for a benefit;
- The request is malicious in intent and being used to harass an organisation. For example, the individual:
  - Explicitly states in communications that they intend to cause disruption;
  - Makes unsubstantiated accusations against specific employees which are clearly prompted by malice;
  - Targets a particular employee against whom they have a personal grudge;
  - Systematically sends different requests as part of a campaign, with the intention to cause disruption

A request may be considered 'manifestly excessive' when it is clearly or obviously unreasonable and the ICB Corporate Governance team will review whether the request is proportionate when balanced with the burden or costs involved in dealing with the request.

The ICB needs to be assured that they know the identity of the requester (or the person the request is made on behalf of) and if unsure, the ICB can ask for further information to verify an individual's identity, and in some cases their authority to request data on behalf of another individual. The ICB will be unable to acknowledge and process the request until the requested information is received. The ICB Information Rights team will close a request where this information has not been received within 60 days.

### **6.3 Time Limits for Compliance with Requests**

BNSSG ICB has procedures in place to ensure it complies with the duty to respond to requests within the statutory timeframe of one calendar month. The deadline can be extended by a further two months if the request is complex or a number of requests have been received from the individual. The ICB will inform the requester of any delays within one month of receiving the request, explaining why the extension is necessary and agree a new deadline.

To manage the flow of information necessary to meet timescales ICB departments may be required to release information internally in advance of any required evidence being produced demonstrating consent. Evidence of consent which may include Lasting Power

of Attorney (LPA) documentation will be necessary before information is released by the ICB.

#### **6.4 Charging a Fee**

Individual rights requests are free of charge however the ICB may in some circumstances be able to charge a fee such as for a repetitive request. The reasonable fee will be based on the administrative costs of complying with the request. Where the ICB decides to charge a fee, the individual will be contacted within one calendar month to inform them of the cost. The request will not be processed until the fee has been received.

#### **6.5 Verifying Identity**

The ICB is responsible for ensuring it is reasonably satisfied of the identity of the requester and will take appropriate steps to ensure this. The ICB will only request information that is necessary to confirm identity and where teams within the ICB already hold identification/authentication documents, these will be reviewed rather than contacting the requester for these documents again.

For children and vulnerable adults the ICB Information Rights team will always seek confirmation of identity.

The ICB will let the individual know without undue delay that more information is needed from them to confirm their identity. The ICB does not need to comply with the request until the additional information has been received.

#### **6.6 Retrieving Information**

When a request is received the ICB will ask the requester to outline the services that they have used which may hold their information to determine which teams to contact for information. Where this information is not provided, the ICB will make reasonable efforts to conduct a search for the information. The ICB is not required to conduct searches that are unreasonable or disproportionate to the importance of providing access to the information.

#### **6.7 Redaction of Third Party Data**

Data subject to Subject Access Requests (SAR) often contains the personal data of another individual and in these cases the data must be reviewed before disclosure. Data Protection legislation states that an organisation does not need to comply with a SAR if doing so identifies another individual.

In most cases it is possible that the third party data can be redacted and therefore not included within the response. Where the data is the personal data of both the requester and the third party, the applicants rights of access must be weighed against the third parties right to privacy. The ICB Information Rights team will consider whether:

- The other individual has consented to the disclosure
- It is reasonable to comply with the request without the individuals consent

The ICB makes a record of all redactions and inclusions of third party data within SAR responses and as part of this the Information Rights team records any consent by the third party as well as any consideration taken as part of the reasonableness tests to include the third party personal data.

There is additional guidance provided by the ICO on the reasonableness of releasing the personal data of a healthcare professional without consent. Personal data of a health worker can be disclosed without consent, if it meets the 'health data test':

- A health record contains the information; and
- The third-party individual is a health professional who:
  - Compiled the record;
  - Contributed to the record; or
  - Was involved in the requester's diagnosis, care or treatment

A health record:

- Consists of data concerning health; and
- Is made by or on behalf of a health professional in connection with an individual's diagnosis, care or treatment

It is also considered reasonable to disclose information relating to third party personal data where:

- the requester has already received the information
- the requester already knows the information
- the information is generally available to the public

Where third party data is redacted from a response, this is communicated to the requester as part of the response letter.

## **6.8 Special Cases: Health Records**

Special rules apply when providing right of access to information about an individual's physical or mental health or condition likely to cause serious harm to them or another person's physical or mental health or condition. In this case the information is likely to be exempt as its disclosure would be likely to cause such harm. In order to apply this exemption there needs to be an assessment undertaken by a clinician to decide whether the exemption applies. The requirement to consult does not apply if the individual has seen or knows the information concerned.

If the Information Rights team identify any such information, the ICB Caldicott Guardian will be consulted on and make the decision on any exemptions.

A further exemption applies where a SAR is made about an individual from a third party who has the right to make the request, such as a parent or someone appointed to manage the affairs of an individual who lacks capacity. Personal data is exempt from the

right to access where the individual has made it clear that they do not want the information to be disclosed to that third party.

From age 13, children are considered mature enough to make decisions regarding their data and therefore must provide consent if their parent or guardian applies for access to their data. It is for the ICB to decide whether a child is mature enough to make decisions regarding their data.

## **7 Access to Health Records Act 1990**

Right of access to records of the deceased is provided under the Access to Health Records 1990. Under the terms of the Act, access is only granted if the requester is:

- A personal representative (the executor administrator of the deceased person's estate)
- Someone who has a claim arising from the death

Details of the documentation required to open an Access to Health Records request is outlined in Appendix 6.

It is accepted that the confidentiality obligations owed by health professionals continue after death. Where the individual requesting the data does not have a statutory right of access under the Act then the ICB would consider whether the disclosure is appropriate and lawful. The following needs to be considered in these cases:

- Preferences expressed by the deceased prior to death
- Any distress or detriment that a living individual may suffer following disclosure
- Any loss of privacy that might result
- The impact on the reputation of the deceased that might result
- The wishes of surviving family
- Length of time after death
- Whether the request is for full or partial disclosure of data

Each case must be considered on a case by case basis and should not be dismissed if the above conditions under the Act are not met.

## **8 Requests for information made on behalf of an Individual**

Under Data Protection legislation, a rights request can be made on behalf of another individual with their consent, or from someone who has the right to make a request, such as a parent or someone appointed to manage the affairs for an individual who lacks capacity. In these cases, consent will be requested from the data subject alongside proof of identity and authority for the requester. Where the requester has the right to make a request without consent, there are a number of considerations taken by the ICB and documents requested. These have been outlined in appendix 6.

The ICB will ask third parties who hold an LPA for the data subject to provide a code for the Office of Public Guardian website which will allow the ICB to review the LPA online. It



has been requested that the code be received to provide added assurance that health data is being released legally. This applies to LPAs registered after 1<sup>st</sup> September 2019.

## **9 Training requirements**

All staff are required to complete training using the NHS Data Security Awareness Level 1 modules provided by NHS Digital (Information Governance Training) or approved face to face training (if offered). Bespoke training on Individual's Rights will be provided to relevant teams and staff by the ICB Corporate Governance team with support from the SCW CSU Information Governance team where appropriate.

## **10 Equality Impact Assessment**

Equality Impact Assessment Screening has been completed and is included at Appendix 1. Screening indicates that a full assessment is not required.

## **11 Implementation and Monitoring Compliance and Effectiveness**

An implementation plan has been prepared and is attached at appendix 2. Compliance with this policy and associated legislation will be monitored by reporting to the Audit and Risk Committee, including information regarding the number of requests received, the percentage responded to within the legislated timeframe and the number of exemptions applied.

## **12 Countering Fraud, Bribery and Corruption**

The ICB is committed to reducing fraud in the NHS to a minimum, keeping it at that level and putting funds stolen through fraud back into patient care. Therefore, we have given consideration to fraud and corruption that may occur in this area and our responses to these acts during the development of this policy document.

## **13 References, acknowledgements and associated documents**

The following related documents may be accessed through our website:

BNSSG Information Governance Policy

BNSSG Records Management Policy

BNSSG Freedom of Information Policy

BNSSG Disciplinary Policy

<https://bnssgICB.nhs.uk/>

The following are additional references associated with this policy:

Data Protection Act 2018

<https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

General Data Protection Regulations (GDPR)

<https://www.legislation.gov.uk/eur/2016/679/contents>

Access to Health Records Act 1990

<https://www.legislation.gov.uk/ukpga/1990/23/contents>

Freedom of Information Act 2000

<https://www.legislation.gov.uk/ukpga/2000/36/contents>

In addition, consideration will also be given to all applicable Law concerning privacy confidentiality, the processing and sharing of personal data including:

- the Human Rights Act 1998,
- the Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015,
- the common law duty of confidentiality and
- the Privacy and Electronic Communications (EC Directive) Regulations
- the ICO Guidance for Individual Rights [A guide to individual rights | ICO](#)

## 14 Appendices

### 14.1 Equality Impact Assessment

Other documents required to complete the Equality & Health Inequality Impact Assessment:

- [Equality & Health Inequality Impact Assessment Guidance](#)
- [Equality & Health Inequality Impact Assessment Resources](#)

Title of proposal: Individual Rights Policy				Date: 17/10/23
<input checked="" type="checkbox"/> Policy	<input type="checkbox"/> Strategy	<input type="checkbox"/> Service	<input type="checkbox"/> Function	<input type="checkbox"/> Other ( <i>please state</i> )
EHIA type:	Screening EHIA <input checked="" type="checkbox"/>	Full EHIA <input type="checkbox"/>	HEAT in progress/ completed <input type="checkbox"/>	Has an EHIA been previously undertaken? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> EIA undertaken on previous policy version
Is the policy under:	Development <input type="checkbox"/>	Implementation <input type="checkbox"/>	Review <input checked="" type="checkbox"/>	
Which groups will this service/proposal impact (e.g. patients, service users, carers/family, staff, general public, partner organisations)?				
All BNSSG ICB employees and members of the public				
Lead person(s) completing this assessment: Lucy Powell				
Lead person job title(s) and service area: Corporate Support Officer				

#### Briefly describe the proposal

*Give a brief description of the context, purpose, aims and objectives of the proposal. Describe what services are currently being provided. Describe the intended outcomes and benefits and who these might impact. Include whether it is a new proposal or change to an existing one and the key decision that will be informed by the EHIA (e.g. whether or not to proceed with the proposal to publish an employee handbook)*

This is an update to the current Individual Rights policy in line with best practice and national guidance. The aim is to ensure that all ICB employees understand the arrangements that BNSSG ICB has in place for the management of individual rights requests. This policy also outlines how members of the public and ICB staff can exercise their individual rights, including the information required by the ICB to process requests.
Health inequalities (HI) are systematic, avoidable and unjust differences in health and wellbeing between different groups of people. Reducing health inequalities improves life expectancy and reduces disability across the social gradient. What health inequalities have or might emerge and what actions can you take to

reduce or eliminate them? Include details of any evidence, research or data used to support your work, e.g. JSNA, ward data, meeting papers, NICE etc below. You can also consider completing the <a href="#">HEAT tool</a> to support summarising key issues, this can help to systematically evaluate HI:
This policy will not directly impact Health Inequalities. However, the ICB does not undertake equality monitoring of requesters and therefore there is no data which shows whether those with protected characteristics are more/less likely to request their data.
Give details of any relevant patient experience data or engagement that supports your work and where there is significant impact and major change how have patients, carers or members of the public been involved in shaping the proposal. Note, where the proposed change results in significant variation public consultation is required, seek advice from your PPI team. If you have not undertaken any engagement, state how you will involve people with protected characteristics or vulnerable groups in the project or explain why there is not likely to be any involvement.
N/A The policy describes the ICB’s statutory and legal responsibilities and there had been no engagement with patients/members of the public in preparing this policy beyond that undertaken by the government as part of the legislative process
Has the project/service ensured that they have/will comply with the Accessible Information Standards (AIS)? Yes or No Describe how the project/service will ensure staff are in compliance and have a consistent approach to identifying, recording, flagging, sharing and meeting the information and communication support needs of patients, service users, carers and parents, where those needs relate to a disability, impairment or sensory loss. For more information on AIS please refer to and <a href="#">NHS England » Accessible Information Standard</a> and <a href="#">AIS at NBT - YouTube</a> .
The policy has been written with a view to be accessible to all individuals and can be requested in other formats as per ICB processes. The policy has been included on the ICB website, and further information about requests has been included on the Contact Us webpage. Additional information for staff is on the intranet and sent out regularly through the newsletter.

**Could the proposal have a positive or negative impact on any of the protected characteristic groups or other relevant groups?**

Although some of your conclusions will be widely known and accepted (e.g. need for accessible information), your analysis should include evidence to support your statements to aid the decision-maker – references and links to documents can be listed in section 4.1. Evidence might include insights from your engagement, focus groups, stakeholder meeting notes, surveys, research paper, national directives, expert opinion etc. If there is insufficient evidence, state this and include an action to find out more in the action plan in Step 3. In addition to having due regard for the Equality Act 2010 Public Sector Equality Duty to eliminate unlawful discrimination, advance equality and foster good relationship between protected groups; you must also have due regard to the principles of the Armed Forces Act 2021 including regarding the unique obligations and sacrifices they make, removing disadvantage and making special provision to ensure services and employment opportunities are accessible.

Positive Impact:				
<input type="checkbox"/> Sex	<input type="checkbox"/> Race	<input type="checkbox"/> Disability	<input type="checkbox"/> Religion & Belief	<input type="checkbox"/> Sexual Orientation
<input type="checkbox"/> Age	<input type="checkbox"/> Pregnancy & Maternity	<input type="checkbox"/> Marriage & Civil Partnership	<input type="checkbox"/> Gender Reassignment	<input type="checkbox"/> Armed Forces <input type="checkbox"/> Other health inequality (please state below)

## Individual Rights Policy

<p>Provide a narrative about the benefits including benefits to any of the protected characteristic groups plus health inequality groups (such as digital exclusion). Also include intersectional impact where possible here:</p> <p>There is no positive impact on those holding protected characteristics. The policy outlines the arrangements that BNSSG ICB has in place for the management of individual rights requests. This policy also outlines how members of the public and ICB staff can exercise their individual rights, and the policy outlines the information required by the ICB to process requests. As per legislation, individual requests can be requested in writing or verbally to anyone in the organisation. The policy also contains the provision for third parties to request and support individuals to receive their data if they are unable to do so themselves. The Policy also includes promotion of the right for individuals not to be subject to automated decision making and profiling. This protects individuals from organisations carrying out solely automated decision-making that has legal or similarly significant effects.</p>				
<b>Negative Impact</b>				
<input type="checkbox"/> Sex	<input type="checkbox"/> Race	<input type="checkbox"/> Disability	<input type="checkbox"/> Religion & Belief	<input type="checkbox"/> Sexual Orientation
<input type="checkbox"/> Age	<input type="checkbox"/> Pregnancy & Maternity	<input type="checkbox"/> Marriage and Civil Partnership	<input type="checkbox"/> Gender Reassignment	<input type="checkbox"/> Armed Forces <input type="checkbox"/> Other health inequality (please state below)
<p>Provide a narrative about the negative impact for any of the protected characteristic groups plus health inequality groups (such as digital exclusion). Also include intersectional impact where possible here:</p> <p>It is not believed that the content of the policy would have a direct negative impact on those holding protected characteristics. The ICB has a duty to provide the policy and information requested in various formats as required to ensure equitable access to the information within the policy and equitable access to information. (you can share further details and mitigations below in 2.2)</p>				
<b>No Effect</b>				
<p>Your policy might not have a positive or negative impact, or it might maintain a status quo – complete this section if ‘not applicable’</p> <p>This EHIA is being undertaken as part of the review process for a current ICB policy. There have been no significant amendments made to the processes already in place.</p>				

**Outline any negative impacts of the proposal on people based on their protected characteristic or other relevant characteristic. Consider how you might level the ‘playing field’ for all people**

Protected Characteristic(s)	Details of negative impact (e.g. access to service, health outcome, experience, workforce exclusion)	Identify any mitigations that would help to reduce or eliminate the negative impact

N/A		
-----	--	--

**Outline any benefits of the proposal for people based on their protected or other relevant characteristics?**

*Outline any potential benefits of the proposal and how they can be maximised. Identify how the proposal will support our Public Sector Equality Duty to:*

To eliminating discrimination, harassment and victimisation.	Positive	X
	Negative	<input type="checkbox"/>
	No effect	<input type="checkbox"/>
Please describe: This policy outlines the individual rights which can be exercised by both staff and members of the public. The rights provide people with access to their personal data, as well as the right to correct data, erase data, restrict processing and the right to object. These rights support the understanding of how the ICB uses and processes personal data which supports individuals to have more control over and understanding of their data. The rights outlined in the policy also encourage transparency and staff are aware that any personal data may be requested and provided to the individual.		

To advance equality of opportunity between people who share a protected characteristic and those who don't	Positive	X
	Negative	<input type="checkbox"/>
	No effect	<input type="checkbox"/>
Please describe: The policy applies to all the individuals equally. The aim is to ensure that everyone understands the arrangements that BNSSG ICB has in place for the management of individual rights requests and provides clear guidance to staff who may have to process requests and members of the public who may want to request information. The UK GDPR outlines that requests can be made verbally or in writing.		

To foster good relations between people who share a protected characteristic and those who don't (e.g. does the project raise any issues for community cohesion, or linked to current topics that are contentious in society; will it affect relationships between any groups)	Positive	<input type="checkbox"/>
	Negative	<input type="checkbox"/>
	No effect	x
Please describe:		

**Action Plan**

**What actions will you take to mitigate the negative impact outlined above?**

Action	Timeframe	Success Measure	Lead
--------	-----------	-----------------	------

## Individual Rights Policy

Senior support and promotion of the policy	From ICB Board approval on the 1 <sup>st</sup> February 2024	ICB Board approval and subsequent promotion at staff meetings and through staff newsletters	RH/LP
Promotion of individual rights on the ICB website	Ongoing	Individual rights requests continue to be received through the contact us page on the webpage	LP

### How and when will you review the action plan (include specific dates)?

As part of the quarterly promotion of the policy and as part of the quarterly reporting to the Audit and Risk Committee

### What are the main conclusions of this Equality & Health Inequality Impact Assessment?

Share a brief summary of the positive impact the project will make and any negative impact and mitigations, e.g. what steps you have been taken to improve accessibility, and what recommendations you are making to the decision maker.

Explain how the EHIA has informed, influenced or changed the proposal and include a recommendation for the decision maker:

The policy is for all individuals including all ICB staff and members of the public. The arrangements outlined are a legal requirement. The EHIA has highlighted the importance of promotion of the policy.

<b>Select a recommended course of action:</b>	
<b>Outcome 1:</b> Proceed – no potential for unlawful discrimination or adverse impact or breach of human rights articles has been identified. E.g. proposal is not likely to have any detrimental impact on any group	<input checked="" type="checkbox"/>
<b>Outcome 2:</b> Proceed with adjustments to remove barriers identified for discrimination, advancement of equality of opportunity and fostering good relations or breach of human rights articles. E.g. arrangements put in place to produce a BSL video to promote changes to a service	<input type="checkbox"/>
<b>Outcome 3:</b> Continue despite having identified some potential for adverse impact or missed opportunity to advance equality and human rights (justification to be clearly set out). E.g. pilot benefits one neighbourhood due to funding restrictions	<input type="checkbox"/>
<b>Outcome 4:</b> Stop and rethink as actual or potential unlawful discrimination or breach of human rights articles has been identified. E.g. dress code policy discriminates against people who practice particular religions; new service that proposes to detain patient but insufficient evidence of safeguarding or human rights considerations in place	<input type="checkbox"/>

*All Equality & Health Inequality Impact Assessments should be reviewed internally and obtain sign off to show an organisational commitment.*

<b>Reviewer's Feedback (this document should be reviewed by an equality officer or trained project lead/senior manager)</b>
<b>Equality Officer Name:</b>

<b>Equality and Inclusion Team Signature:</b>
Date:

### Equality Delivery System 2022

Equality, Diversity & Inclusion is an evidence-based practice, Healthier Together partners are committed to demonstrating how we have taken steps to improve patient and service user access, experience and outcomes and how we have created an inclusive working environment for our staff, including supporting our workforce to have healthy and fulfilled lives. Please indicate which Domain your project will deliver against:

#### Domain 1 – Commissioned & Provided services

- 1A: People can readily access the service.
- 1B: Individual people's health needs are met
- 1C: When people use the service, they are free from harm.
- 1D: People report positive experiences of the service.

#### Domain 2 – Workforce health and wellbeing

- 2A: When at work, staff are provided with support to promote healthy lifestyles and manage their long term conditions
- 2B: When at work, staff are free from abuse, harassment, bullying and physical violence from any source.
- 2C: Staff have access to independent support and advice when suffering from stress, abuse, bullying harassment and physical violence from any source (response to Covid-19)
- 2D: Staff recommend the organisation as a place to work

#### Domain 3 – Inclusive Leadership

- 3A: Board members and senior leaders (Band 9 and VSM) routinely demonstrate their commitment to equality.
- 3B: Board/Committee papers (including minutes) identify equality related impacts and risks and how they will be mitigated and managed
- 3C: Board members, system and senior leaders (Band 9 and VSM) ensure levers are in place to manage performance and monitor progress with staff and patients

The policy aims to provide clear guidance to staff on the responsibilities for managing individual rights requests. Having a clear policy in place with support from the appropriate teams supports all three domains. Domain 1 as individual rights support people to understand their health and the NHS. Domain 2 as staff are supported to make individual rights requests and the policy provides clear guidance to support staff to action individual rights requests. Domain 3 as the policy provides a framework for Board/Committee members and senior managers to monitor impact and risk.



### 14.2 Implementation Plan

Target Group	Implementation or Training objective	Method	Lead	Target start date	Target End date	Resources Required
ICB Board	Ensure the ICB Board is aware of ICB's responsibilities and provide assurance that appropriate process is established to ensure legal compliance	Cover paper to the policy to be presented to the ICB Board	Chief of Staff	1 <sup>st</sup> Feb 2024	1 <sup>st</sup> Feb 2024	Staff time, Board members time
Executive Directors	Ensure awareness of responsibilities of ICB process to ensure compliance. This includes the requirement of Director approval processes	Email confirmation of policy implementation to Executive Directors highlighting sign off procedures for requests	Corporate Support Officer	2 <sup>nd</sup> Feb 2024	2 <sup>nd</sup> Feb 2024	Staff time, Executive Director time
Executive Director PAs	Ensure awareness of ICB process and Executive Director approval role in process	Email confirmation of policy implementation to Executive Directors highlighting sign off procedures for requests to be copied into PAs	Corporate Support Officer	2 <sup>nd</sup> Feb 2024	2 <sup>nd</sup> Feb 2024	Staff time
All Staff	Ensure awareness of ICB processes and procedures	<p>Reviewed policy to be placed on website</p> <p>Information about the policy and ICB process to be placed on the Hub and announced at staff meetings</p> <p>Information about the policy and ICB process to be communicated through internal newsletter</p> <p>Data Security Awareness training module to be completed by all staff</p>	Corporate Support Officer	1 <sup>st</sup> Feb 2024	Ongoing	Staff time IG training module

## 14.3 The Individual Rights in more detail

### THE RIGHT TO BE INFORMED (GDPR ARTICLES 12, 13 AND 14)

The ICB must provide individuals with information including (but not limited to):

- A description of the information
- The purposes the information is used for
- Our retention periods for that personal data
- The disclosures that are made or might be made

This is called 'privacy information' or 'Fair Processing Information' and we must provide privacy information to individuals at the time we collect personal data from them. If we obtain personal data from other sources, we must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

#### How and what information should be provided

The information we provide to people must be

- concise,
- transparent,
- intelligible,
- easily accessible, and
- it must use clear and plain language

We put our Privacy Notice on our website. [How we use your information - NHS BNSSG ICB](#)

We review on an annual basis, and where necessary, update our privacy information. We must bring any new uses of an individual's personal data to their attention before we start the processing.

### THE RIGHT OF ACCESS BY THE DATA SUBJECT (SUBJECT ACCESS REQUEST – GDPR ARTICLE 15)

#### What is the right of access?

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information.

#### What is an individual entitled to?

Individuals have the right to obtain the following from the ICB:

- confirmation that we are processing their personal data;
- a copy of their personal data; and
- other supplementary information such as
  - the purposes of processing;

- the categories of personal data concerned;
- the recipients or categories of recipient we disclose personal data to;
- retention period for storing personal data or, where this is not possible, our criteria for determining how long we will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards we provide if we transfer personal data to a third country or international organisation

Much of this supplementary information is provided in our privacy notice.

### **What about requests made on behalf of others?**

Data Protection legislation does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney if the individual lacks mental capacity.

### **What about the records of deceased individuals?**

The Data Protection Legislation only relates to living individuals. However requests for access to personal data relating to deceased individuals can also be made under another piece of legislation – the Access to Health Records Act (AHRA) 1990. The same rules apply regarding 'fees' etc. under Data Protection legislation; however requests under the AHRA must be completed with 40 calendar days instead of 1 calendar month. The request must still be logged and actioned without undue delay.

### **THE RIGHT TO RECTIFICATION (GDPR ARTICLE 16 AND 19)**

Data Protection legislation includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

This right has close links to the accuracy principle of the GDPR (Article 5(1) (d)). However, although we may have already taken steps to ensure that the personal data was accurate when we obtained it; this right imposes a specific obligation to reconsider the accuracy upon request.

### **What do we need to do?**

If we receive a request for rectification we should take reasonable steps to check that the data is accurate and to rectify the data if necessary. We should take into account the arguments and evidence provided by the individual.

### **THE RIGHT TO ERASURE (GDPR ARTICLE 17 AND 19)**

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which we originally collected or processed it for;
- we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;
- we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- we are processing the personal data for direct marketing purposes and the individual objects to that processing;
- we have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- we have to do it to comply with a legal obligation; or
- we have processed the personal data to offer information society services to a child

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the GDPR. For further details about the right to erasure and children's personal data please read the ICO guidance on children's privacy.

### **RIGHT TO RESTRICT PROCESSING (GDPR ARTICLE 18 AND 19)**

Individuals have the right to request the restriction or suppression of their personal data. When processing is restricted, we are permitted to store the personal data, but not use it.

This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information we hold or how we have processed their data. In most cases we will not be required to restrict an individual's personal data indefinitely, but we will need to have the restriction in place for a certain period of time.

### THE RIGHT TO DATA PORTABILITY (GDPR ARTICLE 20)

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Some organisations in the UK already offer data portability through midata and similar initiatives which allow individuals to view access and use their personal consumption and transaction data in a way that is portable and safe. It enables consumers to take advantage of applications and services which can use this data to find them a better deal or help them understand their spending habits.

### THE RIGHT TO OBJECT (GDPR ARTICLE 21)

An individual has the right to object to

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics

### RIGHT NOT TO BE SUBJECT TO AUTOMATED DECISION MAKING AND PROFILING (GDPR ARTICLE 22)

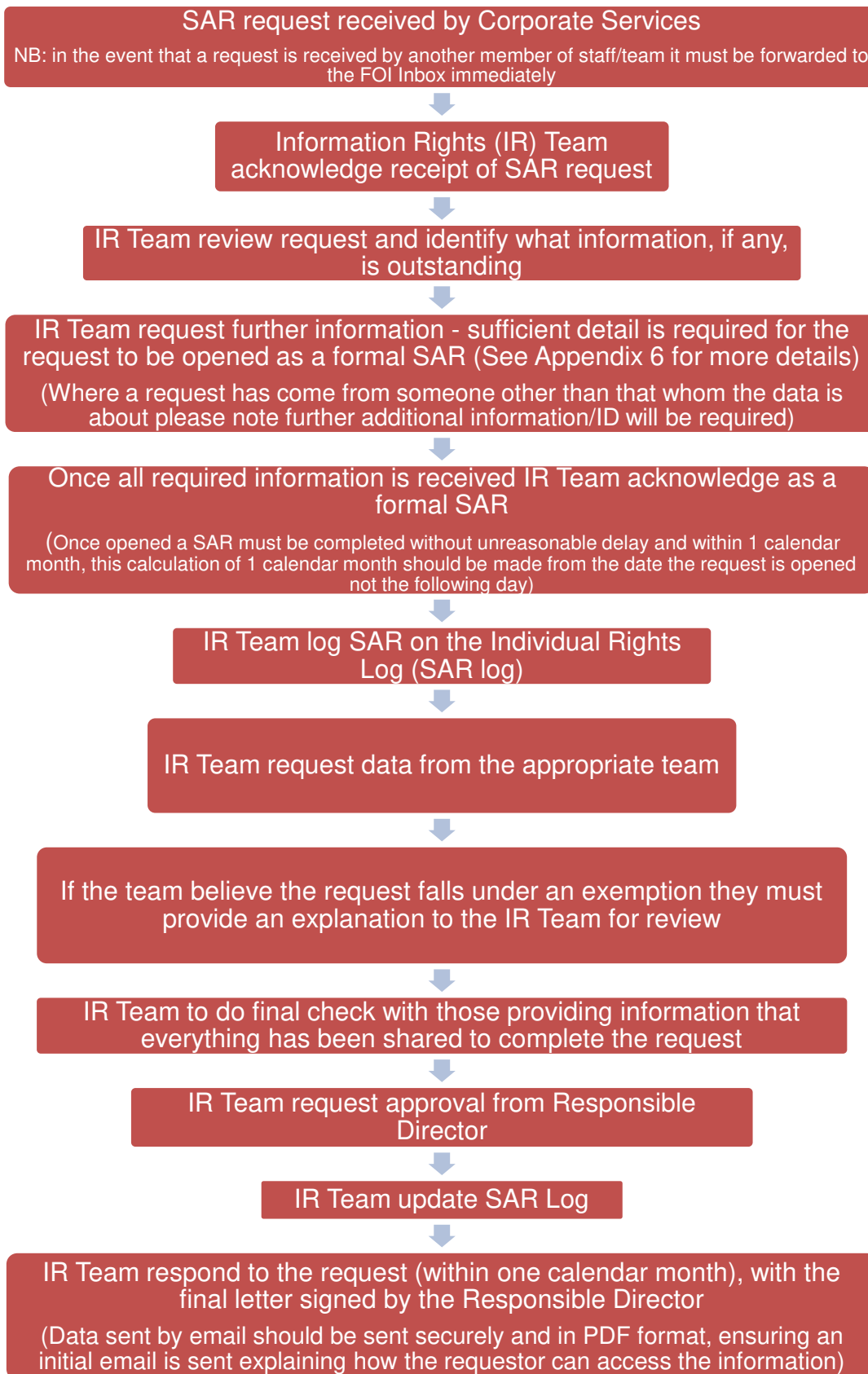
The GDPR applies to all automated individual decision-making and profiling. Article 22 of the GDPR has additional rules to protect individuals if we are carrying out solely automated decision-making that has legal or similarly significant effects on them. The processing is defined as follows:

- **Automated individual decision-making** (making a decision solely by automated means without any human involvement).

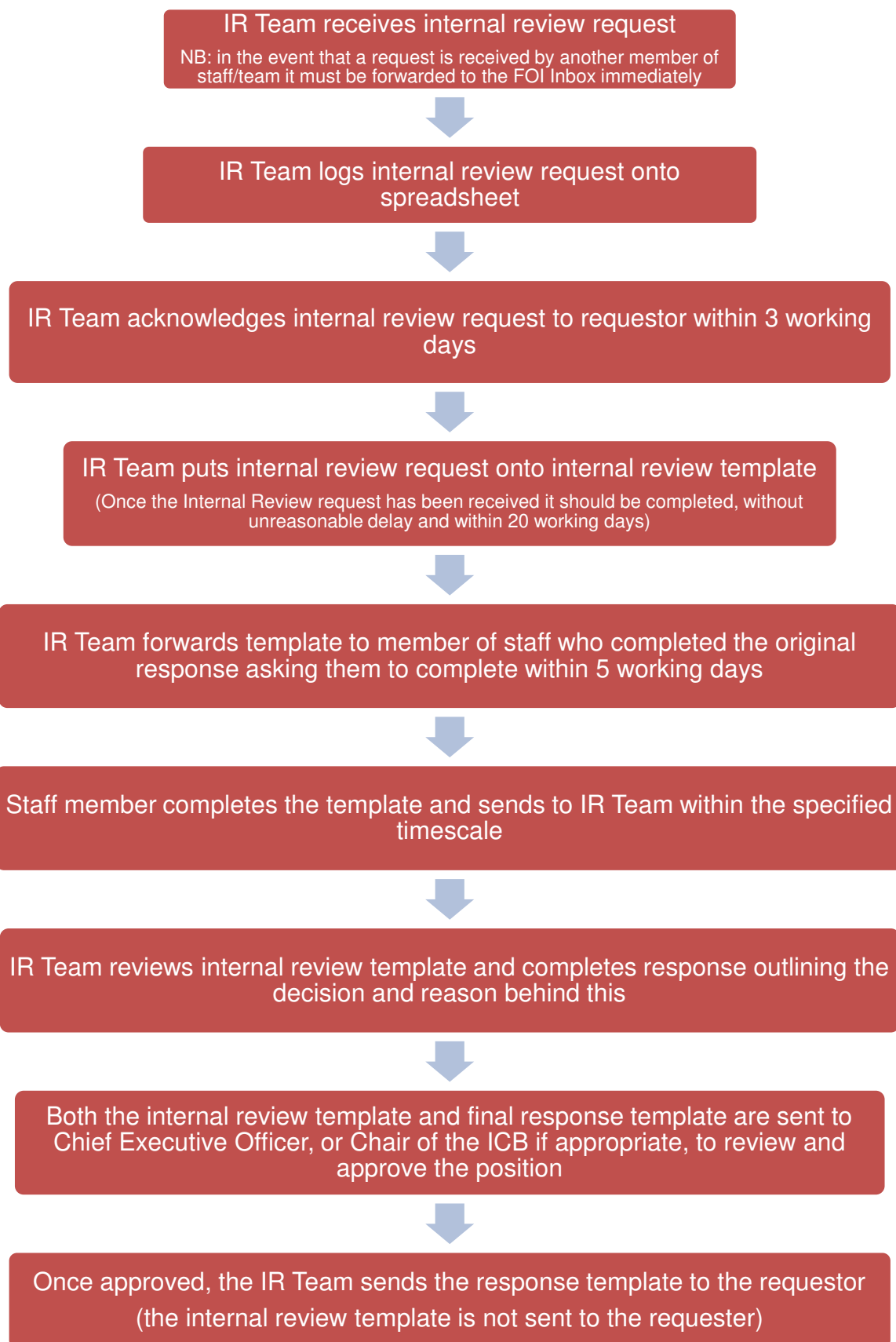
Examples include an online decision to award a loan; or a recruitment aptitude test which uses pre-programmed algorithms and criteria. Automated individual decision-making does not have to involve profiling, although it often will do.

- **Profiling** (automated processing of personal data to evaluate certain things about an individual) and includes any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

## 14.4 Right to Access (Subject Access Request) Procedure



## 14.5 Right to Access (Subject Access Request) Internal Review Procedure



## 14.6 Consent Procedures

Under the Data Protection Act 2018, the act of obtaining consent must not be burdensome for the requester and where possible, the organisation must utilise consent documentation already received through another team rather than ask again. However, the organisation must assure themselves that the appropriate documentation has been received before opening the request.

The Information Rights team have processes in place dependent on the type of information requested and these are outlined below. In all cases, the team undertake sense checks on email addresses and home addresses and check these with any previous communications as well as against the data received to ensure that email and home addresses are consistent.

### Request for own information

Where someone has requested access to their own records the following is requested:

- Name, address and postcode
- The service used which will hold the records
- Any relevant case numbers
- A copy of ID (passport, driving license or birth certificate)
- A copy of proof of address (utility or phone bill from the last 3 months)

The Information Rights team can open a request without proof of address but will not send any information via post without this.

### Request for own information (Child)

Where a child requests their own information, the Information Rights team needs to consider the maturity of the child, the guidance indicates that children over the age of 13 are considered mature enough to request and receive their own records but there will be exceptions. The Information Rights team would request the following information:

- Name, address and postcode
- The service used which will hold the records
- Any relevant case numbers
- A copy of ID (passport, student card etc.)
- A copy of ID containing birth date (birth certificate etc.)

If proof of address was required in order to send the response via post then the team would work with the requester to find a suitable solution for this. These requests would also be further discussed with the team holding the records to understand whether there are any safeguarding issues or concerns.



### **Request for third party information from a solicitor**

Where a solicitor has requested information regarding a third party the following is requested:

- Name, address and postcode
- The service used which will hold the records
- Any relevant case numbers
- Form of Authority signed by the third party

### **Request for third party information (of a child) from an individual**

Where someone has requested information regarding a child the Information Rights team would request the following information:

- Name, address and postcode
- The service used which will hold the records
- Any relevant case numbers
- Proof of relationship to child (birth certificate)
- A copy of ID (passport, driving license or birth certificate)
- A copy of proof of address (utility or phone bill from the last 3 months)
- Dependent on the age of the child, consent from them that the individual could access their records.

These requests will also be further discussed with the team holding the records to understand whether there are any safeguarding issues or concerns.

### **Request for third party information from an individual**

Where someone has requested the information of a third party the following is requested:

- Name, address and postcode
- The service used which will hold the records
- Any relevant case numbers
- A copy of ID (passport, driving license or birth certificate)
- A copy of proof of address (utility or phone bill from the last 3 months)
- Where the third party has mental capacity, consent from the third party must be obtained to include:
  - Name, address and postcode
  - A copy of ID (passport, driving license or birth certificate)
  - Express signed consent for the above individual to receive the records
- Where the third party lacks mental capacity the following is also requested:
  - Relationship to third party
  - Any Lasting Power of Attorney (LPA) documentation (Health and Welfare or Property and Affairs)
  - A copy of the access code to check the status of the LPA on the Office of Public Guardian website (For LPA's issued after 1<sup>st</sup> September 2019).

These requests will be further discussed with the team holding the records to understand whether there are any safeguarding concerns or concerns relating to the individual receiving the records.

It has been agreed that where a third party is requesting data, the consent documentation received will be sent to the team who hold the information so that they can be assured that the consent is in place prior to sending the data to the Information Rights team.

For all third party requests made, following review of the data should there be any indication that the data subject did not wish for part or all of their data to be shared with either anyone or the named requester specifically then the data would not be shared.

### **Request for records of the deceased**

Requests for records of the deceased are processed under the Access to Health Records Act 1990. The Act contains set criteria under which records of the deceased can be released; access is restricted to the patient's personal representative (executor of the will or the administrator of the estate) or any person who may have a claim arising out of the patient's death. Where someone has requested this information the following is requested:

- Name, address and postcode
- The service used which will hold the records
- A copy of ID (passport, driving license or birth certificate)
- A copy of proof of address (utility or phone bill from the last 3 months)
- Where the request is made as a personal representative:
  - Sealed Grant of Probate
  - Valid Will
  - Letters of Administration
- Where there is a claim arising from the patient's death:
  - Evidence of the claim (Solicitors letter or Valid Will)
  - Evidence of relationship with the deceased

It has been agreed that where a third party is requesting data, the consent documentation received will be sent to the team who hold the information so that they can be assured that the consent is in place prior to sending the data to the Information Rights team.

For all third party requests made, following review of the data should there be any indication that the data subject did not wish for part or all of their data to be shared with either anyone or the named requester specifically then the data would not be shared.