NHS
Cornwall and Isles of Scilly

Data protection impact assessment policy and procedure

Date approved: 11 April 2025

NHS Cornwall and Isles of Scilly Integrated Care Board

Call us on 01726 627 800
Email us at ciosicb.contactus@nhs.net
Visit our website: cios.icb.nhs.uk

Part 2S, Chy Trevail,
Beacon Technology Park,
Dunmere Road,
Bodmin, PL31 2FR
Chair: John Govett
Chief executive officer: Kate Shields

Document control sheet

Title of document: Data protection impact assessment policy and procedure
Originating directorate: Transformation and partnerships
Originating team: Information governance
Document type: Policy
Subject category: Information governance
Author(s) name: Bev Gallagher
Date ratified: 11 April 2025
Ratified by: People and organisational governance committee
Review frequency: 3 years (standard, unless otherwise indicated)
To be reviewed by date: 11 April 2028
Target audience: All staff
Can this policy be released under FOI? Yes
Give reasons for exemption if no: N/A

Version control

Version number	Revision date	Revision by	Nature of revisions
V1.0	May 2022	Head of information governance	Working draft awaiting approval
V2.0	17 May 2022	People and organisational governance committee	Policy ratified by the committee
V2.0	1 July 2022	NHS Cornwall and Isles of Scilly Integrated Care Board (ICB)	Policy adopted by NHS Cornwall and Isles of Scilly ICB
V2.0	January 2023	Head of information governance	Rebadged to reflect transition to the Integrated Care Board
V2.1	February 2025	IG Consultant (SCW CSU)	Review and update for DSP Toolkit

Contents

Introduction 4
Purpose 4
What is Privacy 5
Privacy Risk 6
Responsibilities 6
Scope 7
The process 8
Stage 1 – process initiation 8
Stage 2 – DPIA screening 8
Stage 3 – DPIA process queries or changes required 8
Stage 4 – Final assessment 8
Implementation plans and monitoring effectiveness 9
Update and review 9
Regulatory framework 9
ICB related policy documents 10
Appendix 1: DPIA comprehensive assessment 12
Comprehensive data protection impact assessment (DPIA) 12
Data Protection impact assessment screening questions: 12
Step 1 – identify why a DPIA is needed 13
Step 2 – describe the data processing 13
Step 3 – consultation process 14
Step 4 – assess necessity and proportionality 14
Step 5 – identify and assess risks 14
Step 6 – identify measures to reduce risk 15
Step 7a – sign off and record outcomes 15
Step 7b – head of IG/DPO advice 16
Step 7c – SIRO to review and acknowledge residual risks and/or mitigation 16
Key notes: 16
Appendix 2: Equality impact assessment 18
Aims, objectives and purpose of the policy 18
Differential impacts 18
Human rights values 20
Public Sector Value Act 2020 20

Introduction

For many organisations privacy now poses risks which need to be professionally managed in a similar way to other categories of risk. NHS Cornwall and the Isles of Scilly Integrated Care Board (ICB) recognises that handling data is an essential part of their business, and that the introduction of new projects, systems, processes or information flows which include personal data/information need to monitored.

This policy and procedure is designed to illustrate the approach that the ICB is taking regarding monitoring and assessing any changes to person identifiable data/information processing (PID) in the organisation.

It is important to note that any collection, use or disclosure of personal information has the potential to have a risk to personal privacy. Sometimes those risks are not obvious and as a result it can be easy to overlook or not address them properly. Careful analysis at the planning stage of any intended data/information processing changes will be enhanced by the completion of a Data Protection Impact Assessment (DPIA) and must be completed when PID is involved.

The Information Commissioner states, “DPIA’s help identify the most effective way to comply with data protection obligations meet individuals’ expectations or privacy.”

Purpose

DPIAs are used by organisations to identify, understand and address any risks to privacy that might arise when developing new products and services or undertaking any other new activities that involve the processing of PID, particularly on a large scale.

Under UKGDPR Article 35, organisations are legally required undertake DPIAs where their planned processing involves high risk processing.

‘High risk processing’ encompasses activities like:

- automated processing
- large scale processing of special categories data - which includes health and genetic data
- systematic monitoring of a public area, such as using CCTV

Examples include, but are not limited to:

- use of new technologies
- use of profiling or special category data to decide on access to services
- profiling individuals on a large scale
- processing biometric data
- processing genetic data

- matching data or combining datasets from different sources
- collecting personal data from a source other than the individual without providing them
- with a privacy notice (‘invisible processing’)
- tracking individuals’ location or behaviour
- profiling children or target marketing or online services at them or
- processing data that might endanger the individual’s physical health or safety in the
- event of a security breach.

The UKGDPR also requires DPIAs to be undertaken if planned data processing activities are otherwise "likely to result in a high risk to the rights and freedoms of natural persons"

The NHS Data Security and Protection Toolkit (DSPT) also requires NHS organisations to carry out DPIAs as part of Data Protection by Design procedures to ensure that processing is legal, only the minimum necessary personal data is processed and that where possible, data is not identifiable. This is achieved at the planning stage of new information processing. Processing must be transparent and where possible allow individuals to monitor what is being done with their data. Data protection procedures help the organisation to improve data protection and security by preventing any new system or process to begin unless assessments have taken place.

Contracts with third party providers which require the processing of PID are managed to ensure all the necessary standards are met by any service provider. It is the responsibility of the controller to ensure that in such instances a DPIA is created and maintained over the lifecycle of the contract.

It is important that the DPIA process is challenging, probing and systemic and should have the goal of identifying new risks which cannot be dealt with. It is also important that the DPIA forms part of Data Protection by Design and any possible high-risk processing assessment occurs before processing commences.

What is Privacy

Interpreted most broadly, privacy is about the integrity of the individual. However, a DPIA will look to assess the degree to which a proposed processing activity has an impact on individuals’ privacy, assess its compliance with Data Protection and Data security requirements and mitigate identified risks to those individuals. A DPIA should always focus on protecting individuals’ privacy.

Privacy of personal information is referred to either as ‘data privacy’ or ‘information privacy’. Individuals would not expect data/information about themselves to be automatically shared or made available to other individuals or organisations. There is therefore a duty of confidentiality on healthcare organisations to maintain patient privacy unless there is a lawful exception otherwise. Even where data/information is held by

another party, the individual should be able to exercise a large degree of control over that data and its use.

Privacy Risk

Privacy risks fall into two categories. Risks to the individual as a result of disobeying their rights in relation to privacy, loss, damage, misuse or abuse of their personal information. Risks to the organisation as a result of:

- failure to comply with the law, leading to:
- enforcement action; or
- compensation claims from individuals
- retrospective imposition of regulatory conditions
- a failure to meet public expectations on the protection of personal information
- the collapse of a project or completed system
- the costs of redesigning or delaying a system
- perceived harm to privacy
- withdrawal of support from key supporting organisations due to perceived privacy harms.

A DPIA is a systematic process for assessing a proposed process in terms of its impact upon privacy. A DPIA can assist to:

- identify potential issues and concerns on individual or group privacy
- examine how detrimental effects may be overcome
- ensure that new processes comply with privacy law and principles
- avoiding loss of trust and reputation
- avoiding unnecessary costs and inadequate solutions
- assessing risks and implementing appropriate mitigation measures

Responsibilities

The Caldicott Guardian is responsible for protecting the confidentiality of patient clinical information and can provide advice and guidance where the proposed activity involves the collecting, processing, storage and sharing of patient or other personal confidential data. They should be consulted as part of the DPIA process where necessary.

The Senior Information Risk Owner (SIRO) has ownership of the organisations' information risks and provides assurances to the organisations' management team. They have overall responsibility for assessing the risks associated with changes to existing systems or the development of new information systems and can also provide final approval where high risk is identified.

The Data Protection Officer/Head of Information Governance (HOIG) should be consulted as part of the DPIA process to provide specialist advice and guidance relating to the activity and the organisational objectives of its progress. They should also be consulted should any review of a completed DPIA indicate outstanding risks or recommendations that require consideration prior to their acceptance or rejection.

The project sponsor is the individual (often a senior manager or executive) with overall accountability for the project. The project sponsor is primarily concerned with ensuring that the project delivers the agreed business benefits and that the DPIA has been agreed.

All project leads, whether employed by NHS CIOS or as a contracted service such as Cornwall IT Services, are responsible for ensuring that DPIAs are carried out. Project leads must submit DPIAs to the HOIG for all new data/information processes involving person identifiable data (PID).

Information Asset Owners (IAOs) are accountable for the information systems under their control and are responsible for managing any risks associated with data flows into and out of those systems. They are also responsible for the quality, security and confidentiality of any data held in them. They must ensure the need for a DPIA is assessed for all systems, services, projects and programmes, and if required ensure the process is followed.

Information Asset Administrators will:

- ensure that guidance in this document is followed
- recognise actual or potential risks when new processes are being introduced in their directorate / department
- consult with their IAOs and where necessary the HOIG to take steps to understand how to mitigate risks
- encourage project / programme leads to complete the DPIA template at the planning stage of a project / process
- All managers are to be aware of the need for a DPIA's for all new processing involving PID.
- IT security manager is responsible for assessing IT security needs.

All staff employed by the ICB must follow the requirements of this policy and associated policies particularly those relating to information governance and data security.

Scope

This policy and procedure will include any activity that may alter or introduce a new information process that involves, or could contain PID, whether in electronic or paper format.

This policy and procedure will apply across CIOS ICB where PID is managed or processed.

All new PID processing must have an DPIA completed at the beginning of planning or introduction. This will help ensure that Data Protection by Design is effectively implemented and privacy risks are appropriately mitigated before becoming an issue.

The process

Stage 1 – process initiation

The project lead to ensure that the planning documentation includes:

- Full process description
- Stakeholder review
- Necessity and proportionality
- Risk analysis and log

Stage 2 – DPIA screening

The project lead to ensure the completion of:

Initial DPIA comprising 7 sections to be completed (appendix 1) and forward to the HOIG for review.

Stage 3 – DPIA process queries or changes required

HOIG will:

- raise further queries requiring more detailed information and analysis
- suggest project redesign or amendments

If full DPIA is not required for your project, the DPIA must still be considered at all stages of development to which could include a new proposed use of information. Any future *significant* change to the process which would include PID being processed, might require a new DPIA to be completed.

Stage 4 – Final assessment

Final DPIA will contain completed assessments including the data protection compliance check signed by the HOIG.

Highlighted issues and solutions.

The DPIA will then be escalated for approval to the SIRO who will be required to sign off request.

If the DPIA involves the processing of patient personal data of a clinical nature, it must also be reviewed and signed off by the Caldicott Guardian.

The DPIA will be retained by HOIG on behalf of the ICB SIRO. A register of all DPIAs will be created by HOIG and each DPIA logged.

It will be the responsibility of the project lead to review and update the HOIG with any changes which take place at any time during processing.

Implementation plans and monitoring effectiveness

A DPIA must be completed by project leads before any type of PID processing begins which is “likely to result in a high risk”. This means that although the actual level of risk has not yet been assessed project leads must ‘screen for factors that point to the potential for a widespread or serious impact on individuals’. Any high risk processing may require consultation with the ICO.

The HOIG will ensure the policy is made available within the organisation document library and will be included in staff bulletin for wide distribution. Once finalised and approved, all DPIAs will be logged and added to the Data Flow Maps by the relevant Information Asset Owner and included as part of evidence required for the DSPT. The spreadsheet is reviewed and updated annually by HOIG with the assistance of IAOs and project leads identified at the time.

Update and review

Three years or sooner if necessary.

Regulatory framework

Data protection and information governance currently encompasses the following local, national and legal regulations:

Data Protection Act 2018
General Data Protection Regulations
Freedom of Information Act 2000
Human Rights Act 1998
Access to Health Records Act 1990
Computer Misuse Act 1990
Confidentiality: NHS code of practice
BS ISO/IEC 27001 series of information security standards
Caldicott guardian manual and reviews

Common Law Duty of Confidentiality
NHSX Records management code of practice 2021
Health and Social Care (Safety and Quality) Act 2015
Access to Medical Records Act 1988
Copyright, Designs and Patents Act 1988
Copyright (Computer Programs) Regulations 1992
Crime and Disorder Act 1998
Electronic Communications Act 2000
Environmental Information Regulations 2004
Health and Social Care Act 2012
Information security management: NHS code of practice
Regulation of Investigatory Powers Act 2000
Public Interest Disclosure Act 1998
Abortion Regulations 1991
Mental Capacity Act 2005
NHS constitution
Public Records Act 1958
Regulations under the Health and Safety at Work Act 1974
Re-Use of Public Sector Information Regulations 2005
Data security and protection toolkit

The above list is not exhaustive. All legislation can be found here: Legislation.gov.uk

ICB related policy documents

This policy should be read in conjunction with the following policies and documents:

Information governance strategy
Data protection policy
Records management policy
Subject access request policy
Pseudonymisation policy
IT security policy and all linked policies
Integrated identity management policy
Email policy
Disciplinary policy and procedures
Acceptable use policy
Safe haven policy
Data quality policy
Business continuity plans
Risk management strategy and policy
Incident management policy
Freedom of information policy
ICB privacy notice

Home working policy
Information sharing protocols and agreements
Serious incident policy
Confidentiality code of conduct for employees
Data Protection Impact Assessment policy and procedure

This list is not exhaustive. ICB policies can be found here: Policies and procedures - NHS Cornwall and Isles of Scilly (icb.nhs.uk)

The following are the main publications referring to security and confidentiality of personal identifiable information:

- Caldicott reviews UKCGC | The UK caldicott guardian council UKCGC | The UK Caldicott Guardian Council
- Employee code of practice (Information Commissioner) The employment practices code (ico.org.uk)
- NHSX records management code of practice 2021 https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care
- ISO/IEC 27001:2005 and 17799:2005 Information Security Standard ISO - ISO/IEC 17799:2005 - Information technology — Security techniques — Code of practice for information security management ISO - ISO/IEC 27001 and related standards — Information security management
- DSPT - Data Security and Protection Toolkit (dsptoolkit.nhs.uk)

Appendix 1: DPIA comprehensive assessment

Comprehensive data protection impact assessment (DPIA)

A DPIA must, as a minimum, contain:

1. A thorough description of the planned processing operations and the purposes of the processing including, where applicable, the legitimate reasons for processing the data.
2. An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
3. An assessment of the risks to the rights and freedoms of data subjects.
4. The measures intended to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the General Data Protection Regulations (UKGDPR) with regard to the rights of data subjects and other persons concerned.

“The national data opt-out allows a patient to choose if they do not want their confidential patient information to be used for purposes beyond their individual care and treatment - for research and planning.”

Area and/or function DPIA covers: Click or tap here to enter text.
DPIA completed by: Click or tap here to enter text.
Job title: Click or tap here to enter text.
Department: Click or tap here to enter text.
Date: Click or tap here to enter text.

Data Protection impact assessment screening questions:

Answering ‘yes’ to any of these questions is an indication that a DPIA is a necessary exercise. You can expand on your answers as the project develops if you need to. You can adapt these questions if necessary for unusual circumstances.

Questions	Yes/No
Will the project involve the collection of new information about individuals?	
Will the project compel individuals to provide information about themselves?	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	

Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	
Will the project require you to contact individuals in ways which they may find intrusive?	

Step 1 – identify why a DPIA is needed

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA (for example the use of patient identifiable information).

Click or tap here to enter text.

Step 2 – describe the data processing

1. Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

Click or tap here to enter text.

2. Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Click or tap here to enter text.

3. Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? Do we have a known legal basis for processing the data?

Click or tap here to enter text.

Suggested legal basis for processing (see “Key notes” on final page):

Click or tap here to enter text.

4. Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for the organisation?

Click or tap here to enter text.

Step 3 – consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it is not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Examples:

- Head of information governance
- IT security experts in acute provider
- Any third party processor
- Patients/clients/service users
- General public
- Patient representative groups
- CITS or technical experts

Click or tap here to enter text.

Step 4 – assess necessity and proportionality

How are you minimizing the amount of personal data for the use?

Click or tap here to enter text.

Step 5 – identify and assess risks

As a minimum, please ensure the following areas are covered. The list is not exhaustive.

- Where and how will the data be received and stored?
- Is the information backed up?
- Who has access and is the level of access controlled at an individual level?
- How is the information distributed?
- Is a contract or data sharing agreement (DSA) needed and if so, is it in place?
- Is a business continuity plan (BCP) needed and if so, is it in place?
- Is information transferred outside of the UK?
- Is there an agreed data disposal/retention period? How is data disposed of appropriately?

Click or tap here to enter text.

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks, as necessary. *(Please add more rows, if needed)*	**Likelihood of Harm** (Remote, possible or probable)	**Severity of Harm** (Minimal, significant or severe)	**Overall Risk** (Low, medium or high)
1.			
2.			
3.			
4.			

Step 6 – identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in Step 5. *(Please add more rows, if needed)*	**Effect on risk** (Eliminated, reduced or accepted)	**Residual risk** (Low, medium or high)	**Measure approved** (Yes/No)
1.			
2.			
3.			
4.			

Step 7a – sign off and record outcomes

To be completed by head of department, not the individual completing the form:

Measures approved by (include name and job title): Click or tap here to enter text.
Date: Click or tap to enter a date.
Comments - please ensure actions are integrated back into project plan, with date and responsibility for completion:
Click or tap here to enter text.

Residual risks approved by - name and job title: Click or tap here to enter text.
Date: Click or tap to enter a date.
Comments – if accepting any residual high risk, DPO to consult the ICO before going ahead:
Click or tap here to enter text.

Step 7b – Head of IG/DPO advice

To advise on/ensure compliance and review dates.
Head of IG/DPO advice provided by: Click or tap here to enter text.
Date: Click or tap to enter a date.
Summary of Head of IG/DPO advice - DPO will advise on compliance, Step 6 measures and whether processing can proceed:
Click or tap here to enter text.

DPO advice accepted or overruled by - name and job title: Click or tap here to enter text.
Comments/for what reason:
Click or tap here to enter text.

Consultation responses reviewed by - name and job title: Click or tap here to enter text.
Comments - if the decision departs from individuals' views, explain reasoning:
Click or tap here to enter text.
This DPIA will be kept under review by - name and job title: Click or tap here to enter text.
Expected review date: Click or tap to enter a date.

Step 7c – SIRO to review and acknowledge residual risks and/or mitigation

SIRO provided by: Click or tap here to enter text.
Date: Click or tap to enter a date.
Summary of SIRO - DPO will advise on compliance, Step 6 measures and whether processing can proceed:
Click or tap here to enter text.

Please return completed form to the head of information governance -

Key notes:

Lawful processing of information must be in accordance with one of the reasons given below. Article 6 (1) of the General Data Protection Regulations refers:

a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
d) Vital interests: the processing is necessary to protect someone's life.
e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Appendix 2: Equality impact assessment

An equality impact assessment is used to establish how a policy or similar document may impact on individuals, communities, or equality groups to identify and minimise or remove any disproportionate impact. A full impact assessment should be undertaken for policies, strategies, procedures, or projects which are anticipated to have an impact on members of the public. Read guidance on how to complete this document.

Name of policy or service to be assessed: Data Protection Impact Assessment policy and procedure
Department or section: Information governance
Date of assessment: 9 May 2022
Person(s) responsible for the assessment: Head of information governance
Is this a new or existing policy? New

Aims, objectives and purpose of the policy

Describe the aims, objectives, and purpose of the policy.
To make all staff aware of need to complete a Data Protection Impact Assessment and assess risk of processing.

Who is intended to benefit from this policy, and in what way?
Staff will be assured of their compliance with data protection law. Organisation will be assured of consideration of information processing risks and compliance with data protection law.

What outcomes are wanted from this policy?
All person identifiable data will have a legal basis and risks mitigated. Compliance with data protection law.

What factors or forces could contribute or detract from the outcomes?
There is a requirement for data privacy to be risk assessed and evidenced provided to support the submission of the annual DSPT toolkit.

Who are the main stakeholders in relation to the policy?
Staff and the organisation.

Who implements the policy, and who is responsible for the policy?
Head of information governance

Differential impacts

Does this have a positive or negative impact on people who have a black, asian and minority ethnic (BAME) background? How will any negative impact be mitigated?

There is no positive or negative impact identified. The policy applies to all staff employed by the ICB.

Does this have a positive or negative impact on people who identify as male, female or intersex? How will any negative impact be mitigated?
There is no positive or negative impact identified. The policy applies to all staff employed by the ICB.

What is the positive or negative differential impact on people from the perspective of disability? How will any negative impact be mitigated?
There is no positive or negative impact identified. The policy applies to all staff employed by the ICB.

Does this have a positive or negative impact on people who identify as heterosexual, lesbian, gay, bisexual, pansexual or asexual? How will any negative impact be mitigated?
There is no positive or negative impact identified. The policy applies to all staff employed by the ICB.

What is the positive or negative differential impact on people from the perspective of age? How will any negative impact be mitigated?
There is no positive or negative impact identified. The policy applies to all staff employed by the ICB.

What is the positive or negative differential impact on people from the perspective of religion or belief? How will any negative impact be mitigated?
There is no positive or negative impact identified. The policy applies to all staff employed by the ICB.

What is the positive or negative differential impact on people from the perspective of marriage and civil partnership? This is particularly relevant for employment policies. How will any negative impact be mitigated?
There is no positive or negative impact identified. The policy applies to all staff employed by the ICB.

Does this have a positive or negative impact on people who identify as trans or transgender, non-binary, or gender fluid? How will any negative impact be mitigated?
There is no positive or negative impact identified. The policy applies to all staff employed by the ICB.

Does this have a positive or negative impact on people who are pregnant, breast feeding mothers, or those on maternity leave? How will any negative impact be mitigated?
There is no positive or negative impact identified. The policy applies to all staff employed by the ICB.

Are they any other identified groups? How will any negative impact be mitigated?
There are no other identified groups. There is no positive or negative impact identified. The policy applies to all staff employed by the ICB.

Human rights values

How have the core human rights values of fairness, respect, equality, dignity, and autonomy been considered in the formulation of this policy, service, or strategy?
This policy adheres to the core values of human rights in particular the right to privacy and family life.

Which of the human rights articles does this document impact?

☒ To life
☐ Not to be tortured or treated in an inhuman or degrading way
☐ To liberty and security
☐ To a fair trial
☒ To respect for home and family life, and correspondence
☐ To freedom of thought, conscience, and religion
☐ To freedom of expression
☐ To freedom of assembly and association
☐ To marry and found a family
☐ Not to be discriminated against in relation to the enjoyment of any of the rights contained in the European Convention
☐ To peaceful enjoyment of possessions

What existing evidence (either presumed or otherwise) do you have for this?
Data Protection law is underpinned by the rights of individuals to have privacy and respect in the processing of their personal information. Personal data relates to living individuals. The Human Rights Court has also previously stated that personal data protection is “of fundamental importance” to the enjoyment of our right to privacy and family life.

How will you ensure that those responsible for implementing the policy are aware of the human rights implications and equipped to deal with them?
Data protection law is the basis for the Data Protection Impact Assessment and the need to consider all potential data protection risks.

Public Sector Value Act 2020

The ICB is committed and obliged to fulfil the requirements of the Public Sector Social Value Act 2012. This Act requires the organisations to consider how services commissioned or procured might improve the economic, social, and environmental wellbeing of an area.

Please describe how this will support and contribute to the local system, wider system, and community.
Please consider the inclusion of small medium size enterprises (SMEs) in the process and supply chain; economic – promote skills, tackle worklessness, maintain employment, increase volunteer hours to support the community and promote inclusion; social – reduce anti-social behaviour, tackle exclusion by promoting inclusion including to vulnerable groups and environmental – support local, reduce congestion.

Describe how the policy contributes towards eliminating discrimination, harassment, and victimisation.
Does this make the system fairer? Does it challenge, positively change the culture?

Describe how the policy contributes towards advancing equality of opportunity.
Are you using positive action to increase inclusion? Is this helping groups who may be less often heard?

Describe how the policy contributes towards promoting good relations between people with protected characteristics.
Does it educate, integrate, support?

If the differential impacts identified are positive, explain how this policy is legitimate positive action and will improve outcomes, services and or the working environment for that group of people.
N/A

Explain what amendments have been made to the policy or mitigating actions have been taken, and when they were made.
Click or tap here to enter text.

If the negative impacts identified have been unable to be mitigated through amendment to the policy or other mitigating actions, explain what your next steps are using the following equality impact assessment action plan.
The action plan should be completed below if the equality impact assessment has identified that additional steps need to be taken to address adverse outcomes for protected groups, or to collect additional evidence to inform the analysis. Please list below any recommendations for action that you plan to take because of this impact assessment.

Signed (completing officer): Head of information governance
Date: 21 December 2022
Signed (head of department or section): Head of information governance
Date: 21 December 2022

Please ensure that a signed copy of this form is sent to both the corporate governance team with the policy and the equality and diversity lead.