BrisDoc Patient care by people who care

NHS

Data Protection by Design

Version:	Owner:	Created:
3.0	Deb Lowndes (Head of Business Information and Projects)	1st October 2012
Published:	**Approving Director:**	**Next Review**
17th April 2025	Rhys Rhys Hancock (Director of Nursing, AHPs and Governance)	17TH April 2027

Contents

1. Introduction

BrisDoc Healthcare Services will in respect of all personal information implement appropriate technical and organisational measures which are designed to ensure data protection and safeguard an individual's rights.

With a new plan or project, we will ensure we implement these measures at the outset, and these will form an integral part of any Data Protection Impact Assessment (DPIA). We will ensure that only personal data which is necessary for each specific purpose is processed.

Both at the time of the first occasion of processing any personal data and on all future occasions of processing all members of staff must give consideration to the following questions:

1. Is it necessary to collect all the personal data or can the purpose be achieved without certain personal data?
2. Can the purpose be achieved in another way which means that personal data is not required or there is a reduction in the amount of personal data collected?
3. Are we ensuring that the data is being collected for the original purpose only?
4. Are we able to anonymise or ensure pseudonymisation of personal data?
5. Do we continue to require the personal data held or can some or all of the personal data be deleted? *Note - When deleting personal data, it is essential to comply with our Retention and Deletion Policy.*
6. Is the sharing of personal data with other members of the organisation necessary to enable them to undertake their role and would they be unable to do so without processing the personal data?
7. Is the sharing of personal data with other organisations or individuals who are not members of staff of BrisDoc Healthcare Services necessary and:
    - There is information in our privacy policy detailing this sharing.
    - Where appropriate we have entered into a data sharing agreement with the external organisation or individual, or
    - Where appropriate we have entered into a data processor agreement.

Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of BrisDoc.

An essential requirement for any change management control system is the establishment of an accurate and up to date Information Asset Register which lists all of the information systems, current data depositories and data bases used in the delivery of the service. It is vitally important that all such assets have identified Information Asset Owners (IAO) who are responsible for maintaining appropriate standards of confidentiality, integrity, and accessibility and ensuring that data quality is not adversely affected by any changes. IAOs are responsible for any inward and outward flows, managing risks and ensuring that any new systems or changes to systems are assessed for privacy compliance prior to implementation. In order to adhere to good practice for the management of information assets this document establishes a formal mechanism for the approval of new assets and potential changes to existing assets and processes. This will ensure that any security, confidentiality, data protection and data quality issues have been considered for any new or re-configured asset, system or procedure.

By completing the Change Notification Form (Appendix A) and completing the Information Governance (IG) Checklist (Appendix B) an initial compliance assessment of privacy risks and liabilities will then have been conducted. The need for a more detailed Privacy Impact Assessment (PIA) can then be made.

2. Scope of the Procedure

The document covers procedures to be adopted when any significant change or addition is made to BrisDoc's information assets and systems, including: operating systems, application systems, hardware and data collection systems and clinical changes which impact on activity.

The policy applies to all members of staff (including consultant, contract, agency) engaged by BrisDoc.

The policy covers changes which will have an effect on information systems (paper and electronic) which could include installing a brand-new system (hardware/software), replacing an existing system or upgrading operating systems, or a significant change to collection processes. An example of a major change would be the introduction of a new data warehouse, introducing a new GP portal to an existing warehouse, commissioning an external company to provide a service or process data on behalf of BrisDoc.

3. Purpose of the Procedure

The purpose of the procedure is to ensure that any changes to services are communicated and managed and consideration has been made to compliance with confidentiality, data protection and data quality requirements.

The document sets out a simple, but formal, process that requires managers and project managers to notify intended changes to the Information Governance Board, through the completion of the Change Notification Form (Appendix A). The process then requires the manager responsible for system implementation to assess any significant gaps by completing the IG Checklist See Appendix B. This will reveal the areas for further work or development.

The initial assessment of privacy risks and liabilities will indicate whether a Privacy Impact Assessment (PIA) is required. PIA is a process which helps assess privacy risks in the collection, use and disclosure of information. They are recommended where new and intrusive technology is used or where private or sensitive information which was originally collected for a limited purpose is going to be re-used in a new and unexpected way. Guidance is provided in the PIA handbook produced by the Information Commissioner's Office (ICO).

4. Responsibilities

4.1 The Senior Information Risk Owner (SIRO) has ownership of the organisation's information risks and provides assurances to the Board. The SIRO is responsible for assessing the risks associated with changes to existing systems or the development of new information systems and for providing final approval.

4.2 The Information Governance Board (IGB) must be consulted during the design phase of any new service, process or information asset and be made aware of any risks associated with the development. They will formally approve any IG components of the development, including the PIA. This will ensure that the SIRO can provide the necessary assurances to the Board.

4.3 The Information Asset Owners (IAOs/Information Governance Leads) are accountable for the information systems under their control and are responsible for managing the risks associated with any data flows into and out of those systems and for the quality, security and confidentiality of any data held in them.

4.4 It is important that the following roles are consulted when planning change as they offer the best knowledge of a planned, new or existing information asset, its intended purposes and its operating environments. It is therefore important that:

The **Information Governance Board** should be involved to ensure compliance with confidentiality and data protection issues. They will consult and seek approval from the Caldicott Guardian regarding the exchange and use of personally identifiable data and the need for Information Sharing Agreements if appropriate.

The **Business Information Analyst** should be involved to ensure account is taken of potential impacts on the integrity and quality of the information.

The **Programme and Service Director** should be involved at an early stage in the development of new or re-configured electronic systems to ensure the selected security controls are identified, implemented properly and tested.

4.5 All staff members who may be responsible for introducing changes to services, processes or information assets must be informed effectively about the requirement to seek approval from the group that considers information governance compliance issues.

5. Record Keeping and Auditing of Changes to Systems

An audit trail will be kept. Each change will have a form which will record progress at every stage. The form will be the basis of the final implementation change control decisions process.

6. Procedure Awareness

It will be the responsibility of the Information Governance Board to make sure that all relevant managers are aware of the procedure, explain its implications and ensure that it is made available on the intranet and shared drives as appropriate.

7. Privacy assessment

Privacy impact assessments (PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective PIA will allow organisations to identify and fix problems at an early stage,

reducing the associated costs and damage to reputation which might otherwise occur. PIAs are an integral part of taking a privacy by design approach.

Data Protection Impact Assessments (DPIAs) are mandatory when you wish to implement a new plan or project which might result in a risk to personal data. The process of completing a DPIA is designed to help you to identify and then minimise what risks there may be to data.

The template in Appendix A should be used to complete a DPIA.

Before completing this DPIA it is suggested that you read this policy fully and the Data Protection Policy.

You should also notify your *SIRO and/or DPO* of the project and for advice.

All the questions in the DPIA may not be relevant to your project, but you should still consider them. If they are not relevant, we suggest you mark as “not applicable” (N/A), to show you have addressed the question.

Once completed, the final stage is to carry out a risk assessment using the scoring tables in the DPIA Policy, Appendix B will aid the completion of this.

The template is required to be reviewed by your SIRO and/or DPO and the outcome reported to the IG Board.

If the DPIA is accepted a copy of the DPIA should be stored with project materials and within the Information Governance folders as a new asset.

The template can be found in the Information Governance folders or required from BrisDoc’s SIRO.

Data Protection Impact Assessments (DPIAs) are mandatory when you wish to implement a new plan or project which might result in a risk to personal data. The process of completing a DPIA is designed to help you to identify and then minimise what risks there may be to data.

In addition to a DPIA it some circumstances it will be helpful to consider/complete the Equality Impact Screening matrix

8. Monitoring and Control

The Information Governance Board will monitor the introduction of new services and the compliance with the procedure. Failure to use the procedure will be recorded and appropriate follow-up action taken.

Appendix A –Data Protection Impact Assessment Template.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

1. Introduction

Name of project	
Link to any wider project	
Date project due to commence	
Date DPIA commenced	
Date DPIA completed	

2. DPIA Project Team

Name	Organisation	Role	Contact Details

3. Review and Approval

Detail who will be involved in review and approval of the DPIA					
Name	**Organisation**	**Role**	**Review**	**Approval**	**Email**

4. DPIA Description and Objectives

Describe the project, giving background and technical information where necessary. Explain what you are trying to achieve including your objectives, the purpose, the reason and the benefits of the project to individuals and other parties. If helpful, attach project proposal.

5. The Data Subject

Categorise your data subjects and identify which individuals will benefit from the project and which individuals may be adversely affected. It may be helpful to consider.	**Risk Type**
5.1 Will you have new data subjects? •	
5.2 Will children be included in the new data subjects? •	
5.3 How many data subjects will be affected by this project? • •	•
5.4 Would the data subjects expect you to use their data in this way? •	•
5.5 What control will the data subjects have over the data being processed?	
5.6 Will the project result in you making decisions or taking action around individuals in ways which could have a significant impact on them?	

5.7 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 are likely to consider as private?	
5.8 Will the project require you to contact individuals in ways which they may find intrusive?	
Additional Information	

-

- **6. Your Lawful Basis/es for Taking the Data**

6.1 List your lawful reason(s) under Article 6 UK GDPR. Consider the lawful reasons below. Mark as "not applicable" (N/A) those which are not relevant and expand on those you are using.	**Risk Type**
a) Consent - explain how this will be recorded. What steps will be taken if consent is withdrawn or withheld?	
b) Contract – give details of the contract.	
c) Legal obligation - provide details	
d) Vital interests – provide details	
e) Public interest – provide details	

f) Legitimate interest – provide details	
6.2 If you are to process special category data what is your lawful basis? Delete those which are not relevant and expand on those you are using. •	•
a) The data subject has given explicit consent	•
b) Necessary for the purposes of carrying out obligations in the field of employment, social security and social protection law	•
c) Necessary to protect the vital interests of the data subject or another person	
d) Processing in the course of the legitimate interests of a foundation, association or not for profit body with a political, philosophical, religious or trade union aim, with the data not being disclosed outside the organisation	
e) Processing data which has been made public by the data subject • •	•
f) Necessary for taking or defending legal claims • • •	•
g) Necessary for substantial public interest •	•
h) Necessary for preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care, or treatment or the management of health or social care systems • • •	•

i) Necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices. • •	•
j) Necessary for archiving purposes in public interest, • scientific or historical research purposes or statistical purposes • • •	•
6.3 If you are to use electronic means for marketing such as email, text or phone have you obtained the appropriate positive opt-in in order to comply with the Privacy and Electronic Communication Regulation 2003? Set out how this will be achieved.	

7. Describe the Data you are taking

List the categories of data you are taking and set out the reasons for requiring that data. Examples of data:

Types of Data	Reasons for taking	Risk Type
a) Name •	• •	• •
b) Address •	•	a
c) Email •	• •	• •
d) Phone number •	•	a

e) Date of birth •	•	a
f) Next of kin or family details	•	a
g) Employment history •	•	a
h) Payroll number •	•	a
i) Driving Licence Number	•	a
j) NHS number •	•	a
k) Organisation security number	•	a
l) National Insurance Number	•	a
m) Education and professional training	•	a
n) Financial information eg bank account/credit card	•	a
o) Social services benefits	•	
p) Social circumstances	•	
q) Other	•	
r) Other	•	
s) Other	•	
t) Other	•	
u) Other	•	

8. Data Protection by Design

Give consideration to whether all the data and the processing of data is necessary. You may wish to consider:	Risk Type
8.1 Is all the data relevant to your purpose? •	
8.2 Could you achieve your purpose with less data?	
8.3 Could you anonymise the data?	

8.4 Necessity and Proportionality **Describe compliance and proportionality measures, in particular:** •	•
a) Is there another way to achieve the same outcome? • •	•
b) How will you ensure data quality and data minimisation?	
c) What information will you give individuals? •	•
d) Do all the recipients need to receive/have access to the data? • •	•
e) What measures do you take to ensure processors comply?	
f) How do you safeguard any international transfers? Do you need to make any at all? •	•

9.Describe the Processing of the Data

A. <u>Describe the type of processing.</u>	**<u>Risk Type</u>**
9.1 Identify the source of the data eg individuals or a third party.	
9.2 Explain how you will collect, use, store and delete the data.	
9.3 Consider the 6 principles set out in Article 5 GDPR: •	
a) Is the processing fair? •	
b) Does the data subject know what you are doing with their data? Provide details •	

c) Is the data being collected for a specified and legitimate purpose? Provide details	
d) Will you further process the data which is incompatible with the original purpose? If yes, provide details •	
e) Is the type of data necessary for the purpose you are trying to achieve? Provide details • •	
f) Is the data sufficient for what you are trying to achieve? Provide details • •	
g) Is the data adequate to achieve the purpose? Provide details •	
h) Is the data relevant to the purpose? Provide details • •	
i) Have you limited the data to that which is necessary? Provide details •	
j) Is the data accurate? *Consider carefully if the data is from a third party*	
k) Have you decided on a retention period? Provide details	

l) What processes will be in place to delete data when it is no longer required.	
m) Do you have appropriate security to prevent unauthorised or unlawful processing of the personal data? Provide details •	
9.4 How will the data be stored?	
9.5 How long will you keep the data?	
9.6 Is the project for the processing of a significant amount of personal data on individuals or groups of individuals? If yes, provide details	
B. <u>Describe the nature of the processing</u> •	**<u>Risk Type</u>** •
9.7 Is the processing a change from existing processing? •	•
9.8 What is the source of the data? •	•
9.9 How will you collect the data? •	•
9.10 How many individuals are affected? •	•
9.11 What geographical area does it cover? •	•
9.12 How will you use the data? •	•

9.13 How often will the data be collected? •	•
9.14 Will you be sharing the data? If yes, with whom and why. ***Consider principle of transparency and if you require a data sharing agreement.*** •	•
9.15 Will other organisations be involved in the processing of the data? If yes, state who and why? ***Consider a data sharing agreement or processor agreement*** •	•
9.16 What processes will be in place to delete the data?	•
9.17 Are any processes high risk?	•
9.18 Is the process new for example a new database or a paper process replaced by an electronic one? •	•
9.19 Is the supplier fully compliant with the data protection legislation? Provide details of the steps taken to determine this.	•
9.20 Consider if the data will be processed outside the EEA and if so what measures are in place to ensure UK GDPR compliance • •	•

10.Use of New Technologies and areas of High Risk

	Why Necessary	**Risk Type**
a) Systematic and extensive Profiling with significant effects		
b) Automated Processing		

c) Large scale use of special category data		
d) Data relating to criminal convictions		
e) Monitoring of the Public		
f) New Technologies eg facial recognition		
g) Biometric data		
h) Genetic data		
i)Denial/change of service		
j) Privacy Intruding		
k) Data matching		
l)Invisible Processing or tracking		
m)Targeting of children or other vulnerable individuals		
n)Risk of physical harm when a data breach		
o) Any other relevant details		

11.Confidentiality

Consider whether there are issues of confidentiality which affect the processing of the data. You may wish to consider: •	**Risk Type**

a) **Does confidentiality affect the way in which you are proposing to process the data?** • •	•
b) **Does confidentiality affect the provision of personal data to others?**	
c) **Will there be processing of personal data on a large scale which could impact on the confidence of the data subjects in relation to security of confidential information?** •	

12.Data Flows

It is important to map the data flow to illustrate the source, how it will pass through your organisation and the security measures in place.					
Flow name	**Going from**	**Going to**	**How transferred**	**Security measures in place**	**Where stored after use**

13.Context of the Processing

It is important to understand the context for this project. Consider the nature of your relationship with the data subjects, how much control they will have, if there have been concerns over a project of this nature previously.	**Risk Type**
13.1 The nature of your relationship with the data subject	
13.2 How much control will the data subject have?	
13.3 Is it likely that the data subject will have concerns over the data to be taken and the method of processing?	

13.4 Are there prior concerns over this type of processing or security flaws?	
13.5 Is it unusual in any way?	
13.6 What is the current state of technology in this area?	
13.7 Are there any issues of public concern which should be factored in?	
13.8 Are you signed up to an approved code of conduct or certification scheme?	
13.9 Will you be using a Data Processing Agreement? If yes, give full details of why and what steps you had to take to ensure protection of data to include a contract with the processor.	
13.10 Will this result in data being processed outside the EEA? If yes, what security steps have you taken?	

14.Security

Provide details of how the personal data will be kept secure. You may wish to consider respect of all aspects of IT and paper: •	**Risk Type**
a) IT Software security provisions	
b) Audit trails of user activity	
c) Encryption	
d) Backup •	
e) Secure cabinets •	
f) Business continuity plans •	

g) Cyber security measures •	
h) Cyber essentials •	
i) Cyber Insurance	
Comments	

15.Consultation

Consider if the project will impact on individuals, stakeholders or a partner organisation's data and privacy risks and whether any other person/organisation needs to be consulted/notified. This could be internally or externally.		
15.1 Consider whether you need to consult IT experts or any other expert?		
Name	**Reason to notify/consult**	**Action**
15.2 Have you consulted your DPO?		
Name	**Reason to notify/consult**	**Action**
Provide details of outcome of consultation		

16. Information Technology

List details of any electronic equipment/software to be used			
Name of software	**How it will be used**	**The supplier**	**Who is responsible**

17.Data Subjects Rights

It is important to ensure that the rights of the data subject are not compromised. How does the project impact on those rights? If you are using new software consider the impact on those rights?
17.1 right to access
17.2 right to rectification
17.3 right to erasure
17.4 right to restrict processing
17.5 right to data portability
17.6 right to object

18. Reviewing and Scoring – See Schedule 1

Describe the source of the risk, which could be an individual or non-human, and the nature of the potential impact on individuals. Examples will include unauthorised access to data, accidental loss of data, discrimination, financial loss, reputational damage, restriction on rights. **By using the risk scoring tables in your DPIA policy assess and score your answers above, using the formula likelihood + impact = risk type.** **By way of example, if the likelihood is unlikely and impact is minor that would be a risk type of 4 which equals a moderate risk.** **Once you have calculated the risk type, you need to mitigate any high risks or extreme risks or alternatively report them to the ICO.** **Your DPO will assist you on mitigation on dealing with high or extreme risk**

19.Identify Measures to Reduce Risks

If applicable, identify additional measures you could take to reduce or eliminate risks. This could include training or future security testing or limiting access to the data. ***Refer to the details given above in order to reach these conclusions.***

Risk	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated/reduced	**Residual risk** Low/medium/high	**Measure approved** Yes/No

20.Training

Identify what training needs are required and of whom to ensure full implementation of the project and data protection awareness		

Area of Training	Individuals to be Trained	Person Responsible for Training

21.Conclusion

All privacy risks have been identified and actions completed to mitigate, accept or remove the risks – as specified in this document at Sections 18 and Schedule 1
It is essential that having identified the risk the final impact on the data subject after implementing each solution is a justified, compliant and proportionate response to the objectives of the project.

Where the processing remains a high risk that cannot be mitigated the ICO must be consulted.

Item	Name	Date	Notes
Is it necessary to notify the ICO? If so who is responsible?			
Measures approved by:			Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:			If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided			DPO should advise on compliance, point x measures and whether processing can proceed
Summary of DPO advice:			
DPO advice accepted/not accepted by:			If not accepted, you must give reasons

Explain reasons if DPO advice not accepted			
Consultation responses reviewed by:			If your decision differs you must explain your reasons
Explain reasons if these differ from others' views			
This DPIA will be reviewed by:			The DPO should also review ongoing compliance

22.Integration

List the key individual(s) responsible for integrating the outcomes of the DPIA back into the project and those responsible for implementation.				
Name	**Organisation**	**Role**	**Email**	**Mobile No**

Action to be taken	**Responsibility**	**Date completed**

Schedule 1

Risk Number	Risk Type Rare, Unlikely, Possible, Likely, Almost Certain	Mitigation or Reporting Needed
5.1		
5.2		
5.3		
5.4		
5.5		
5.6		
5.7		
5.8		
6.1a		
6.1b		
6.1c		
6.1d		
6.1e		
6.1f		
6.2a		
6.2b		
6.2c		
6.2d		
6.2e		
6.2f		
6.2g		
6.2h		
6.2i		
6.2j		

6.3		
7.a		
7.b		
7.c		
7.d		
7.e		
7.f		
7.g		
7.h		
7.i		
7.j		
7.k		
7.l		
7.m		
7.n		
7.o		
7.p		
7.q		
7.r		
7.s		
7.t		
7.u		
8.1		
8.2		
8.3		
8.4a		
8.4b		
8.4c		

8.4d		
8.4e		
8.4f		
9.1		
9.2		
9.3a		
9.3b		
9.3c		
9.3d		
9.3e		
9.3f		
9.3g		
9.3h		
9.3i		
9.3j		
9.3k		
9.3l		
9.3m		
9.4		
9.5		
9.6		
9.7		
9.8		
9.9		
9.10		
9.11		
9.12		
9.13		
9.14		

9.15		
9.16		
9.17		
9.18		
9.19		
10.a		
10.b		
10.c		
10.d		
10.e		
10.f		
10.g		
10.h		
10.i		
10.j		
10.k		
10.l		
10.m		
10.n		
10.0		
11.a		
11.b		
11.c		
13.1		
13.2		
13.3		
13.4		
13.5		

13.6		
13.7		
13.8		
13.9		
13.10		
14.a		
14.b		
14.c		
14.d		
14.e		
14.f		
14.g		
14.i		

Appendix B: Risk Assessment Guidance

Risks to Individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Corporate Risks

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.
-

Non-Compliance Risks

- Non-compliance with the DPA.
- Non-compliance with the Privacy and Electronic Communications
- Regulations (PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.

Approaches to mitigating risks

Some of the more likely measures include:

- Deciding not to collect or store particular types of information.
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.

- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's
- behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

Appendix C - Equality Impact Screening Matrix

This equality impact screening matrix is intended to identify if the implementation of a new system being introduced by BrisDoc might adversely affect someone with a protected characteristic and/or risk BrisDoc breaching its Public Sector Equality Duty or fail to comply with the Equality Delivery System. Key criteria will be considered against each protected characteristic and if the implementation of the policy, project etc. would cause, or would have the potential to cause, an adverse impact on the person a full equality impact assessment should be undertaken.

		Yes / No	Comments
1	Does the policy/guidance affect one group less or more favorably than another on the basis of:		
	Age		
	Disability		
	Religion or belief		
	Sex		
	Sexual Orientation		
	Marriage/Civil Partnership		
	Pregnancy and maternity		
	Gender reassignment		
	Race		
2	Is there any evidence that some groups are affected differently?		
3	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?		
4	Is the impact of the policy/guidance likely to be negative?		
5	If so can the impact be avoided?		
6	What alternatives are there to achieving the policy/guidance without the impact?		
7	Can we reduce the impact by taking different action?		

If you have identified a potential discriminatory impact of this document, please progress to undertaking a full equality impact assessment.

Tables

Date	Reviewed and amended by	Revision details	Issue number
Jun-12	DL	First Draft	1.0
Oct-12	DL	Formatting and amendments after first review	1.1
Sep-14	SP	Reviewed – Amended job titles	2
Sep-16	DL	Annual review	2.1
Jul-17	DL	Addition of NHS Vulnerability Assessment Good Practice for infrastructure assessment	2.2
Dec-17	DL	Addition of Equality Impact Screening Matrix	2.3
Apr-18	DL	Update of PIA template	2.5
Nov-18	SP/DL	Routine review and to reflect reference to new DPST and refinement of PIA questions as a result of revised ICO template	2.6
Oct-20	DL	Version reviewed – No amendments	2.7
Feb-22	DL	After DPO review renamed to Data Protection by Design Policy. With the addition of statement to section one introduction.	2.8
March 24	DL	Annual review	2.9
Feb 25	DL	Annual review after change of SIRO, review by DPO update of DPIA template to that provided by DPO	3.0