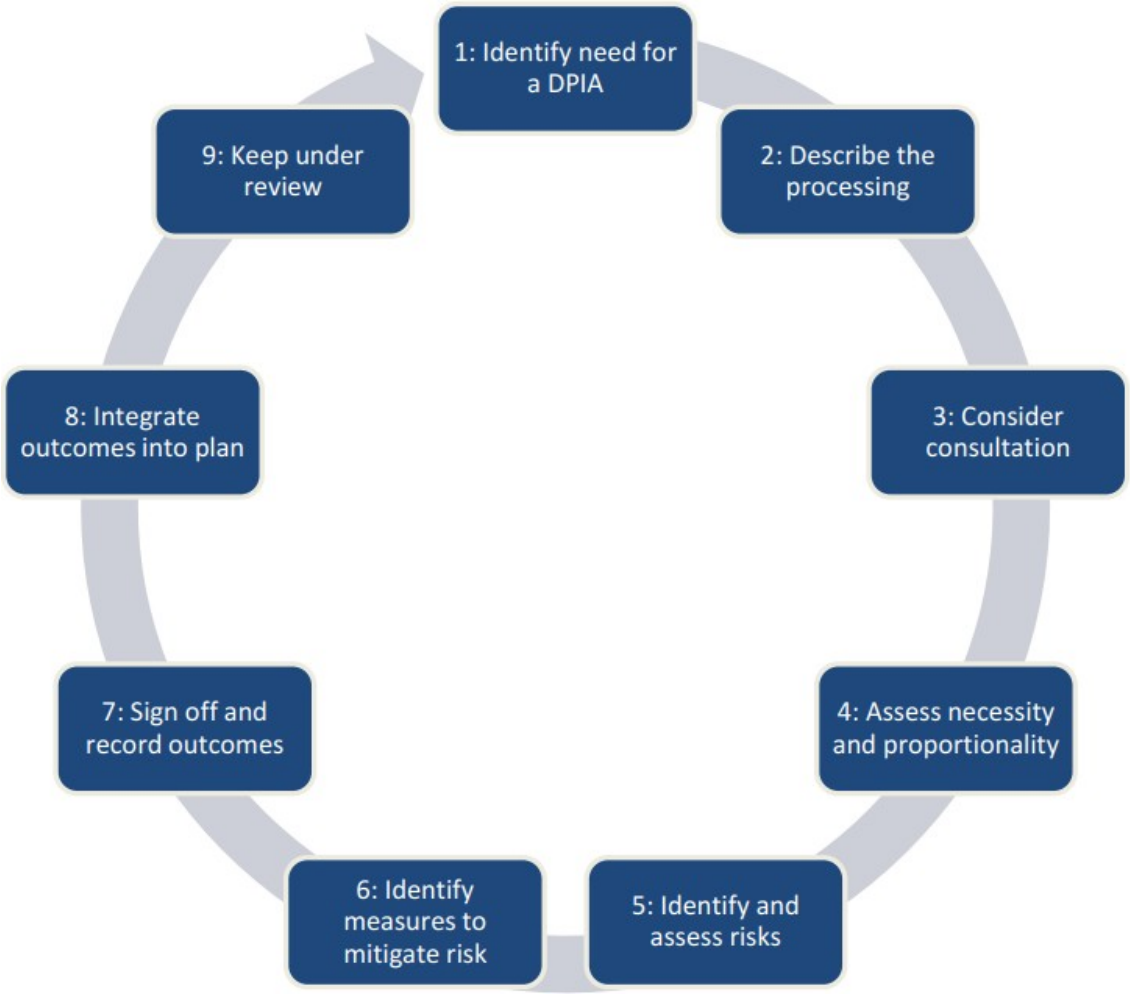
Standard Operating Procedure (SOP)

DATA PROTECTION IMPACT ASSESSMENTS

SETTING	Trustwide
FOR STAFF	All staff involved in managing new or changing personal data handling processes: e.g. Information Asset Owners and Project Leads
ISSUE	Ensuring any new or changed processing complies with Data Protection by Design requirements and is adequately risk assessed

Standard Operating Procedure (SOP)

A data protection impact assessment (DPIA) should begin early in the life of a project, and approval is required before you begin processing, and run alongside the planning and development process. It is an iterative process and includes these steps:



This SOP links with the Data Protection Impact Assessment Workbook held on the DMS: [redacted]

A DPIA is a key tool in ensuring that the Trust complies with requirement of “Data Protection by Design and Default”. This is the aim to consider data protection and privacy issues up front when designing or reviewing any system, service, product or process and that only the required information is processed to achieve the specific purpose of that project.

Step 1: Identify need for a DPIA

Any new or change project that involves the collection, use or storage of personal data requires the completion of the first sections of the Data Protection Impact Assessment Workbook, Background Information and Screening Questions.

UHBW will accept DPIAs completed elsewhere, as long as the necessary information is supplied, and any local impacts have been reviewed.

Research studies that obtain Health Research Authority and Ethics Approvals are judged to have completed the necessary risk assessments, and a separate DPIA is not required.

The Background Information section asks for key contacts and a description of the what project aims to achieve and the necessary data processing to achieve this.

The Screening Questions assess the project against the criteria where the Information Commissioner's Office or the UK General Data Protection Regulation requires a DPIA to be completed. A "Yes" to any of these screening questions will require the completion of the full DPIA.

If all Screening Questions have been answered "No", then save and return the DPIA to Information Governance, who will review and either confirm that no DPIA is required, ask for more information or request that a full DPIA is completed if one of criteria is thought to be met.

Step 2: Describe the Processing

A brief description of the processing will have been completed as part of the Background Information section of the Data Protection Impact Assessment Workbook. The information provided here helps to provide context to the risk assessment.

It is helpful to include information relating to the:

- Nature of processing (what to plan to do with the personal data?)
- Scope of processing (what does the processing cover?)
- Context of processing (what's the wider picture which may affect expectations or impact?)
- Purpose of processing (what is the reason or aim of the processing?)

Step 3: Consider Consultation

With any new or change project, you should consider whether it is appropriate to consult the individuals affected (or their representatives). This can be to understand any expectations or concerns from the affected parties, or if any previous issues can be addressed.

Depending on the processing, you may be required to conduct a more general public consultation process or targeted market research. If the DPIA or processing is then at odds with the consultation results, you will need to explain why the results have been disregarded in Section 6.

Consultation with the Information Governance Team is integral to this process, and they will discuss where further consultations may be required.

Step 4: Assess Necessity and Proportionality

The description of the processing in Step 2 will help to provide the basis to answering the questions assessing whether the data you aim to process is necessary and proportional to achieving your objective. The DPIA Workbook assesses data protection compliance, which is a good measure of necessity and proportionality, particularly:

- Lawful basis for processing (1.2, 1.3-1.10 and 1.11)
- Preventing function or purpose creep (Background Information, Section 1)
- Ensuring data quality (1.16, 1.17)
- Ensuring data minimisation (1.15, 2.3)
- Providing privacy and fair processing information (4.1)
- Supporting individual rights under UK GDPR (4.2-4.4, 4.7-4.9)
- Measures to ensure data processors comply with Data Protection Law (1.20, 1.21, 2.4, 3.1-3.4, 4.2)
- Safeguarding international transfers (3.9)

Step 5: Identify and Assess Risks

Section 5.1 allows for the recording of project specific risks relating to the data processing against the Trust's Risk Management criteria. You should consider the potential impact on individuals and any harm to them which may be caused by on contributed to by the proposed processing, for example:

- Inability to exercise rights
- Inability to access services
- Loss of control over the use of personal data
- Retaining information longer than necessary
- Discrimination
- Identity theft or fraud
- Financial loss
- Reputational damage (to the Trust or individual)
- Physical harm
- Loss of confidentiality
- Reidentification of anonymised or pseudonymised information
- Any other significant economic or social disadvantage or interference with privacy

You should also refer to your answers to 3.5-3.8 and record any specific security risks arising from these. This can include illegitimate access to, modification of or loss of personal data.

You must make an objective assessment of the risks using the Trust's risk assessment matrix, as if there were no controls in place. Any mitigations should then be listed in step 6.

Step 6: Identify Measures to Mitigate Risks

Section 5.2 allows for the recording of mitigations against the inherent risk levels identified in 5.1. Typical options for mitigating data protection risks can include:

- Not collecting certain types of data
- Reducing the scope
- Reducing retention periods
- Additional security measures, including secure disposal/deletion of data
- Training staff

- Anonymising or pseudonymising data where possible
- Writing internal guidance or processes to avoid risks
- Adding a human element to review automated decisions
- Using a different technology
- Putting clear data sharing agreements into place
- Making changes to privacy notices
- Offering individuals the chance to opt out where appropriate
- implementing new systems to help individuals to exercise their rights

You can then record whether the risks have been accepted, reduced or eliminated for discussion with Information Governance prior to DPIA sign off.

Step 7: Sign Off and Record Outcomes

Once you have completed the Background Information, Screening Questions and Sections 1-6, you should submit the DPIA to InformationGovernance@UHBW.nhs.uk for review.

Information Governance will review the provided information and request additional information or clarifications where required or advising on any improvements to the noted information. This may also include circulating the DPIA to specialist teams for their advice before referring a full response back to the Project Lead.

Once all outstanding issues have been resolved, Information Governance will request approval of the DPIA from the corresponding signatory based on the highest level of residual risk identified in 5.2:

Low or Moderate – Data Protection Officer
High – Senior Risk Information Officer and Information Risk Management Group
Very High – The Information Commissioner's Office

Sign off will be recorded by the Information Governance Team and the signed version will be returned to the Project Lead.

Step 8: Integrate Outcomes into the Project Plan

You must integrate the outcomes of the DPIA back into your project plans. You should identify any action points and who is responsible for implementing them. You can use the usual project management processes to ensure these are followed through.

You need to keep your DPIA under review, and you may need to repeat it if there is a substantial change to the nature, scope, context or purposes of your processing. Relevant DPIAs should always be considered by information asset owners when reviewing the ongoing use of the assets for which they are responsible.

DPIAs may be published to aid transparency and accountability, either proactively or in response to Freedom of Information Requests. UHBW aim to publish a summary of approved DPIAs, and any disclosure of completed documentation would be subject to redaction in line with Freedom of Information exemptions.

Appendix 1 – Evidence of Learning from Incidents

The following table sets out any incidents/ cases which informed either the creation of this document or from which changes to the existing version have been made.

Incidents	Summary of Learning
None	

Table A

REFERENCES	Data protection by design and default | ICO Data protection impact assessments | ICO
RELATED DOCUMENTS AND PAGES	[redacted]
AUTHORISING BODY	Information Risk Management Group
SAFETY	None
QUERIES AND CONTACT	InformationGovernance@UHBW.nhs.uk
AUDIT REQUIREMENTS	Review on Information Asset Register to ensure each Information Asset has a completed DPIA – Information Governance, Quarterly

Plan Elements	Plan Details
The Dissemination Lead is:	Information Governance
Is this document: A – replacing the same titled, expired SOP, B – replacing an alternative SOP, C – a new SOP:	A
If answer above is B: Alternative documentation this SOP will replace (if applicable):	N/A
This document is to be disseminated to:	All staff involved in new or change projects
Method of dissemination:	Newsbeat and DMS
Is Training required:	No

Document Change Control

Date of Version	Version Number	Lead for Revisions	Type of Revision	Description of Revision
May 18	1.00	Interim Data Protection Officer	Major	First Draft to include all relevant information to comply with GDPR
May 20	2.00	Information Governance Officer	Major	Review due, updated to reflect merged organisation and new template.
Mar 23	3.00	Information Governance Manager	Major	Review due. Updated to reference new DPIA Workbook criteria and to be more concise. Merged into new template.