



## DATA PRIVACY IMPACT ASSESSMENT DOCUMENT

### Screening Questions

These questions are intended to help you decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be necessary. You can expand on your answers as the project develops if you need to.

Question	Response	
Will the project involve the collection of new information about individuals?	Yes	No
Will the project compel individuals to provide information about themselves?	Yes	No
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Yes	No
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Yes	No
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics, or CCTV.	Yes	No
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	Yes	No
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 very private	Yes	No
Will the project require you to contact individuals in ways that they may find intrusive?	Yes	No

## **Data Privacy Impact Assessment**

### **Step One – Why you are conducting a DPIA**

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

### **Step Two – Describe the information involved**

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of data flows. You should also state how many individuals are likely to be affected by the project.

### **Step Three – Identify the privacy and related risks**

**Principle 1 – Information shall be processed fairly, lawfully and in a transparent manner**

<b>Privacy issue</b>	<b>Comments</b>
Have you identified the purpose of the project?	
How will you tell individuals about the use of their personal data?	
Do you have a Privacy Notice in place to cover the processing of this data? If so does it need to be updated?	
<p>Please tick the data items collected.</p> <p>Personal</p> <p>Sensitive</p>	<p><b>Name</b>  <b>Date of Birth</b>  <b>Address</b>  <b>Post Code</b>  <b>Next of Kin</b>  <b>Sex</b>  <b>National Insurance Number</b></p> <p><b>Sexual Orientation</b>  <b>Religion</b>  <b>Ethnic Origin</b>  <b>Genetic/Biometric</b>  <b>Political Opinions</b>  <b>Physical/ Mental health</b>  <b>Union Membership</b></p> <p><b>Other (please state):</b></p>
Who provides the information?	
Have you established the legal basis for processing? If so, what is it?	
If you are relying on consent to process personal data, how will this be collected and recorded?	
Do you need to validate the age of the data subject and if so, how will this be done?	
Have you checked and confirmed that the data subject has capacity to give consent?	

**Principle 2 – Information shall be collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with the original purpose**

<b>Privacy issue</b>	<b>Comments</b>
----------------------	-----------------

Please state the purpose for the processing of the data: for example, research, audit, service provision	
Which personal data could you not use without compromising the needs of the project?	

**Principle 3 – Adequate, relevant and limited to what is necessary in relation to the purposes**

Privacy issue	Comments
Is the quality of information good enough for the purpose it is used?	

**Principle 4 – Accurate and kept up to date**

Privacy issue	Comments
How are you ensuring that the personal data obtained from individuals or other organisations is accurate?	
How will the information be kept up to date and checked for accuracy and completeness?	
If the data subject withdraws their consent how will this be actioned and recorded?	
Is there a documented process to amend and/or delete data when necessary?	

**Principle 5 - Kept in a form that permits identification no longer than is necessary**

Privacy issue	Comments
What are the retention periods for the data?	
Are you procuring software that will allow you to delete information in line with your retention periods?	
How will the data be destroyed when it is no longer required?	

**Principle 6 - Processed in a way that ensures appropriate security of the personal data**

Privacy issue	Comments
Do the systems provide protection against the security risks identified?	
What training and /or guidance is in place to ensure that staff know how to operate the system securely?	

Is there a useable audit trail in place for the system/asset?	
Where will the information be kept/stored/accessed?	
Will any information be sent off site?  If yes where will it be sent and how will it be transferred?	
Is there an access policy in place which covers the data referred to in the DPIA?	
Is there a contingency plan/back up policy in place to manage the effect of an unforeseen event?	
Are there procedures in place to recover data (both electronic and paper) which may be damaged through human error, computer virus, network failure, theft, fire or flood?	

### **Rights of the individuals**

<b>Privacy issue</b>	<b>Comments</b>
What process is in place to support answering Subject Access Requests?	
Do you intend to send direct marketing messages by electronic means?	
If applicable, are there any procedures in place for an individual to prevent processing for purpose of direct marketing.	
Is automated decision making used?  If yes how will you notify individuals?	
Have you assessed that the processing of personal/sensitive data will not cause any unwarranted damage or distress to the individuals concerned?	
What procedures are in place for the rectifying/blocking of data by individual request or a court order?	
Will the information be shared with any other organisation or third parties?	

**Step 4 – Completion of Risk Assessment and Mitigation**

<b>Risks Identified</b>	<b>Solutions</b>	<b>Evaluation (would the risk eliminated, reduced or accepted?)</b>

**Step 5 – Sign off and record of DPIA outcomes**

<b>Risks</b>	<b>Approved Solution</b>	<b>Approved By</b>	<b>Date Approved</b>

Reviewed and Adopted by Full Council on 22 March 2021  
To be reviewed April 2023