Data Protection Impact Assessment

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Please provide as much detail as possible. When considering the information you will process think about whether the information is necessary for the specified purpose? Is it essential for the successful implementation of the project? If not – then don't collect it.
It will also be useful to describe the information flows – where will the data come from; who receives it – if it is to be disclosed further who will it be sent to and how will it get there. You can append a data flow map to this document.

Project/Lead Details

Project/ Processing Title	
Assessment Completed by	*This should be the Project Lead*
Job Title	
Department	
Contact Number	
Contact email	
Register of Processing ID	*If this is an existing project- you can find this from the intranet under Information Governance & Compliance- "Register of Processing Activities" and filter by Department.*
Submission date to IG&C	
Outcome	*For IG&C Use*
Review Date	*For IG&C Use*

Step 1: Identify the need for a DPIA

Explain broadly what 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.

Step 2: Describe the processing

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 other way of describing data flows. What types of processing identified as likely high risk are involved?	
Source/Collection *Direct from data subject* *Indirectly from another source*	
Usage *Purpose*	
Sharing *Who* *Why* *How*	
Retention/ Destruction *Retention Period* *Anonymization/Destruction Method*	

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?

Specify the type of data that will be collected/shared/used – and explain why each type is required (add as required)

Description of Data	**Why is it Required**
1. **2.** **3.** **4.** **5.**	**1.** **2.** **3.** **4.**
Will the information include any of the following:	**Please tick if yes**
Information relating to physical or mental health	
Information relating to an individual's sexual life	
Information relating to an individual's lifestyle and/or social circumstances	
Information relating to criminal offences or proceedings	
Information relating to the education or training	

Information relating to employment or career history	
Information relating to the financial affairs of the individual	
Information relating to religion or beliefs	
Information relating to any membership of a trade union	
PLEASE NOTE – if the answer to any of these is YES, an additional legal basis (under Article 9 of GDPR) will be required and advise should be sought from the Information Governance & Compliance Department	

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)?

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 you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's 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? It is recommended that you consult with stakeholders throughout this PIA process

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

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

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
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, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA