your coop

Data Protection Impact Assessment (DPIA)

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.
xxx

Step 2: Describe the processing

Describe the nature, scope and purpose of processing here. Consider: How will you use, store and delete data? Will you share data with anyone? (It may be useful to refer to data flow diagram) What are the categories of data (eg name, address, email etc) and does it include special category data (eg health data, race, biometric data etc)? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? Are there prior concerns over this type of processing or security flaws? What will the processing achieve? What are the benefits for the Society and the affected individuals?
xxx

Step 3: Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? (eg. Society's Data Protection Officer or Legal Services, external advisors, industry regulations etc.). How will you carry out the consultation? You should link this to the relevant stages of your project management process. Note: Consultation can be used at any stage of the DPIA's process.
xxx

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 ensure data quality and data minimisation? What information will you give individuals?

What measures do you take to ensure processors comply?

Will there be any international data transfers? What steps will you take to safeguard any international transfers?

Note: Refer to ICO guidance for:
Lawful basis for processing
Conditions for processing Special Category Data

xxx

Step 5: Identify privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks.

Please note the following:
- consider the risks under each of these headings, they do not need to be linked
- larger-scale DPIAs might record this information on a more formal risk register
- If unsure, refer to the Society's risk appetite statement relevant to the type of risk.

For example, the risk appetite statement states: **the Society has a minimal risk appetite to Regulation and Compliance risks.** Overall, we strive to be compliant with all relevant regulatory and legislative requirements. However, in exceptional circumstances the Society will accept that it may be impractical to fully comply with regulation/legislation and will be prepared to accept minimal compliance breaches.

Please identify risks under each of the four headings. Each heading should be considered individually.

Privacy issue	Risk to individuals	Compliance risk (arising from failure to comply with law or regulations, such as GDPR)	Society risk

Step 6: Identify measures to reduce risk

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Note: Please state each risk and the associated mitigation, result and evaluation for that risk.

Risk	**Mitigation**	**Result:** **is the risk eliminated, reduced, or accepted?**	**Evaluation:** **is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the Project?**
xx	xx	xx	xx

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
DPIA approved by COO or Exec:	xx	Ensure actions (including mitigation at step 6) are integrated back into project plan, with date and responsibility for completion
DPO advice provided:	xx	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: xxx		
This DPIA will be kept under review by: This should be the Project Manager in conjunction with DPC for your business area. Escalating to DPO where appropriate.	xxx	The review should be of a) any significant changes in project and b) to ensure adherence to DPIA (including mitigation of risks).