Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

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.

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.
Photographs are to be captured by the Engagement Officers (EOs) as they represent the OPCC in the community. This will include photographs of people, taken at official events. Some of these photographs will be published in the OPCC Annual Report which is a public document. DPIA required due to the possibility of photographs of vulnerable people such as children. Where, for example, reformed ex-offenders are photographed this might constitute special category personal data. It is possible that even uncaptioned photographs could be linked to an identifiable living person through the use of technology or with reference to information elsewhere such as the details of the location or group the photograph represents.

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?
The photographs will be captured using mobile phones while EOs are out and about. They will be captured for the purpose of illustrating the annual report, Police and Crime Plan, OPCC website and possibly other publications and may therefore shared widely.

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?
The data could be used to extrapolate special category personal data such as criminal history. Even if names are not added as captions it is potentially possible to use automated systems that are freely available to identify people. There will be dozens of photographs, although not all are being used. No retention period has yet been agreed. Most photographs will be of residents of the Humberside area.

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)?
The individuals will be coming into contact with the OPCC as part of community engagement activities. Under present circumstances they do not have control of whether or how their images are used. Children and vulnerable groups could be involved, and they may be at Youth clubs or similar groups where their parents are not present to give consent directly.

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?
The purpose is to illustrate the OPCC's reports and to share good news about engagement with our local communities. This will increase public confidence and trust in the Office of the Police and Crime Commissioner and help the public understand how they are represented through the PCC.

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?
Individuals' views cannot be taken as it is not possible to establish a precise sohort that may be involved. The DPO and CEO need to agree on the rules.

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?
Although there is a public interest in sharing the activities of the OPCC, the advice of the OPCC DPO is that the lawful basis for processing this data must be consent. My advice is that: • The verbal or written consent of individuals or group leaders to take photographs must be obtained, along with their contact details. • Data must be stored in filing system that allows for the contact details of the person/s in the photograph to be indexed with each image. • Further consent should be sought before publishing a person's image, and they must be aware whether this will form a printed document or on the open internet and whether the document is for internal use by Criminal Justice Partners or open to the public. • It must be made clear that even if they withdraw consent the documents containing their image may not be able to be fully withdrawn. • They must have the right to refuse consent and once the relevant report has been completed, all unused photographs recorded for that purpose must be securely disposed of or the individuals contacted for consent to store them for possible future use. • To exercise this responsibility I will provide information to the Communications and Engagement Manager to cascade to the team, perhaps as a credit-card sized guide

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
Data breach – loss or theft of device containing photographs	Possible	Significant	Medium
Usage of photographs that person does not agree with and they cannot then be withdrawn.	Possible	Severe	High
Evidence of consent and image become separated or contact details are lost altogether	Possible	Significant	Medium
Images of children or vulnerable people are taken when someone capable of giving consent is not present (such as a parent or carer)	Possible	Significant	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
Data Breach	Only use force-issued secure password protected and encrypted devices to take and store photographs	Reduced	Low	
Unwanted usage of photographs	Record details of people on photograph – or a representative of the group – and seek their consent to take the photograph. Before reusing a photograph, ensure that consent for that specific publication is obtained. Delete all unused photographs after the publication of the report/website content to ensure they are not used without authorization Seek consent for photographs to be stored for potential future use.	Reduced	Low	
Contact Details misplaced or lost	Delete image: do not use it	Eliminated	Low	

Photographs of children or vulnerable people do not have consent of appropriate person	Take consent of group leader if part of an organised group. When asking for consent, make clear that the individual consent of an appropriate adult for each person in the photograph must be sought and recorded. If any person in the photograph refuses consent then do not use the image.	Reduced	Medium	

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Rachel Cook	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:	Mike Richmond 7/8/2019	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Record consent and check before using any photographs. Take special care around children and vulnerable people who may not be able to give informed consent for their photographs to be shared.		
DPO advice accepted or overruled by:	Rachel Cook	If overruled, you must explain your reasons
Comments: This will be implemented from 2020's annual report when the Pentana system is in place to allow contact details to be associated with photographs.		
Consultation responses reviewed by:	N/A	If your decision departs from individuals' views, you must explain your reasons
Comments:		

This DPIA will kept under review by:	Dave Hudson	The DPO should also review ongoing compliance with DPIA