Crime Education 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.
A need for a Crime Education Service was identified following the conclusion of the Not in Our Community (NIOC) contract earlier this year. The new service will be provided by ESKI who provided the previous NIOC contract. Of note the website Not In Our Community – Protection against exploitation. It is expected that the service will go into schools and other educational settings both to deliver the sessions using a train the trainer approach. In addition, children and young people could be involved in the development of content including photographs and used in the production of videos. Content is likely to be available in education settings, social media and websites. As a result of the above it is possible that personal data will be used.

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 data collated such as videos and photos will be collated for the use of a Crime education Service that will be delivered to education settings. The real names of children and young people will not be used instead a pseudonym will be used. Parental / Carer age-appropriate consent will be obtained. The provider will keep the information for the duration of the contract and in line with its document retention policy. The date processed by the provider (mainly for obtaining consent) will be restricted to: Name Name of parent / carer Address Phone Number Date of Birth Email address

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 individuals data that will be processed by the provider will be children and young people in education settings. They will collate basic contact details for the purpose of obtaining consent for their pictures and / or to be used in videos as part of content creation for the Crime Education service.

Data can be collected throughout the 2-year contracts from 01 July 2024 – 30 June 2026.

It covers the four Local Authority areas under the remit of the Police and Crime Commissioner for Humberside. Those being, Hull, East Riding of Yorkshire, North East Lincolnshire and North Lincolnshire.

Data will be kept for the length of the contract, reviewed on a regular basis and destroyed as appropriate as per the providers document retention policy. No criminal offence data will be recorded.

I have considered the following Special Category Data in the table below:

Special Category	**Data collected**	**Special Category**	**Data collected**
Racial or ethnic origin	No	Biometric Data	No
Political opinions	No	Health	No
Religious or philosophical beliefs	No	Sex Life	No
Genetic data	No	Sexual orientation	No
Trade Union Memberships	No		

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 Office of the Police and Crime Commissioner have a 2 year contract in place with the provider ESKI. They will hold the data and this could include children and young people. There is a train the trainer approach in place which could result in OPCC staff also delivering training into schools. Whilst the OPCC will have details of the schools it will not hold personal identifiable data.

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 record those that have agreed to have photos and those have to be agreed to be video's for the purpose of delivering a crime education service that includes the creation of videos that will ab available on social media and lesson plans that will be delivered in schools.

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? Have you consider data ethics implications?
As part of the consultation process the following staff / organisations have been consulted. John Gilbert, ESKI Alice O'Dwyer, ESKI Pip Betts, OPCC-VPP Mike Richmond, OPCC Data ethics implications have been considered, with no concerns identified.

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?
ESKI will need to undertake the following. • The verbal or written consent of individuals or group leaders to take photographs must be obtained, along with their contact details by the provider, ESKI. • Data must be stored in a 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 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. It is expected that the DPO will provide training to relevant VPP and OPCC on the agreed process.

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** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high
Data breach – loss or theft of device containing photographs or video content created.	Possible	Significant	Medium
Usage of photographs that person does not agree with and they cannot then be effectively withdrawn (e.g. as published on internet or permanently retained hard copy document)	Possible	Severe	High
Evidence of consent and image become separated or contact details are lost altogether	Possible	Significant	Medium
Images of children and/or young 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** Eliminated reduced accepted	**Residual risk** Low medium high	**Measure approved** Yes/no
Data breach – loss or theft of device containing personal data	Only use equipment with secure password protected and encrypted devices to take and store personal data. Two way authentication to be considered for extra security.	Reduced	Low	Yes
Usage of content that person does not agree with and they cannot then be effectively withdrawn (e.g. as published on internet or permanently retained hard copy document)	Record details of children and young people, seek appropriate consent. Before reusing a photograph or image 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	Yes

Evidence of consent and image become separated or contact details are lost altogether	Delete image(s): do not use them	Eliminated	Low	Yes
Images of children or vulnerable people are taken when someone capable of giving consent is not present (such as a parent or carer)	Take and record provisional 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/video content refuses consent then do not use the image.	Reduced	Medium	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Leigh Collins 24/07/2024	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 22/7/2024	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: I recommend that although provisional consent can be gained from group leaders, a more granular approach should be taken prior to the dissemination of any images or video footage of participants by means of the provider taking direct consent from the parent or guardian of the data subject. I recommend that the provider are asked to demonstrate their robust consent management processes as part of contract management and that, as with other OPCC contracts, data protection issues and breaches form part of the regular meetings.		
DPO advice accepted or overruled by:	Rachel Cook 24/07/24	If overruled, you must explain your reasons

Comments: I am content that the measures proposed will mitigate risks sufficiently.		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Leigh Collins 24/07/2024	The DPO should also review ongoing compliance with DPIA