DPIA – Community Safety Fund & Community Response Fund

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.
The OPCC uses an external, online platform for funding applications called Good Grants. After the initial applications have been made, it is then necessary to remove data from the online system and process it further, in order to facilitate the decision-making process and to transfer funds to successful applicants. **Lawfulness, fairness and transparency** Data is being collected under the lawful purpose of entering into a contract with the data subject. **Purpose limitation** Data is only to be used for the purpose of processing grant applications and awarding grants. **Data minimisation** The online platform (https://smallgrants.humberside-pcc.gov.uk/) is compliant with the requirements of the UK-GDPR, collecting only enough personal data to process the application, with the lawful purpose of entering into a contract. **Accuracy** Users provide data themselves and have a secure login whereby they can correct any data inaccuracies. **Storage limitation** Personal Data will be retained by the Creative Force (Good Grants system provider) in accordance with their Data Retention Policy available at https://www.creativeforce.team/privacy-policy/ The OPCC has control over the retention of information within its IT system which has been set to 2 years for unsuccessful applicants and 6 years for successful applications.

Integrity and confidentiality (security)

Good Grants is security certified to the requirements of ISO/IEC 2700. Data is stored in the UK, as the system allows users to choose the location of the servers for their dedicated cloud storage.

Accountability

A privacy notice is issued to applicants, which has been reviewed by the Data Protection Officer. The system also has the capability to adjust the privacy notice, retention periods etc. where that is deemed necessary. A Data Processing Contract is in place and stored on the online system.

This Data Protection Impact Assessment is being completed due to the new system, and the need to remove data from it and keep a second copy on OPCC Systems.

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 that is collected comes from applicants direct and is initially stored on Good Grants system. Every application is transferred from this system manually onto the OPCC IT network where it is stored in a shared folder accessible to the entire OPCC Team in unredacted PDF format. It is not shared further. Data flows are shown in Appendix A.

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?
There will be no collection of Special Category Data. It is basic personal details including name, email and phone number. The data will be retained in line with the schema set up within Good Grants for successful/unsuccessful applications in line with the Limitation Act 1980, Data Protection Act 2018 (Subject Access) and the OPCC's obligation as a public authority for transparency under the Freedom of Information Act 2000. In the first two rounds of the Community Safety Fund, we have received 74 and 62 applications respectively. We anticipate similar levels of response for further rounds. The Community Response Fund is likely to have a lot lower level of responses per bidding round, given that the geographical and thematic focus is a lot more specific than the Community Safety Fund.

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)?
Individuals will self-register with the Good Grants system with the intention of applying for funding. All applicants have to be over 16 (18 without parental approval) and this is stated within the Privacy Policy. The processing is otherwise not novel in any way.

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 individuals' contact details are only recorded to process a contract with them (or exclude them from a grant). They stand to gain from the processing through the opportunity to access funding.

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?
No consultation was deemed necessary by the DPO as this is not a fundamentally different process to what came before.

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?
Lawful basis for processing is Performance of a Contract (or steps to enter into one). The processing will achieve this purpose. Data quality is controlled by the applicant when they sign up to the system and data minimization is achieved through discrete fields for information. Individuals are given a link to a privacy policy upon signing up, and are included in the main OPCC Privacy Policy once they have a contract with us.

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
Taking second copy of personal data could affect the integrity, accuracy and/or retention of that data when compared to the data stored in the Good Grants System	Possible	Minimal	Low
Data could be accessed by people within the OPCC other than those named in the data flow	Possible	Minimal	Low
When consulting with other team members about applications, an unredacted PDF will be shared which may contain the applicant's personal data. This could introduce bias to the process.	Possible	Minimal	Medium
An inappropriate person e.g. a child registers with the system in error, or does not go on to make an application.	Possible	Minimal	Low

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
Taking second copy of personal data could affect the integrity, accuracy and/or retention of that data when compared to the data stored in the Good Grants System	1. Regularly check integrity of data (not effective use of time and resource) 2. Make the OPCC copy the master copy once removed from Good Grants	1. Eliminated 2. Reduced	Low Low	No Yes
Data could be accessed by people within the OPCC other than those named in the data flow	1. Restrict access to named individuals and/or role profiles 2. Operate a culture of Trust in line with organizational values	1. Eliminated 2. Reduced	Low Low	No Yes

When consulting with other team members about applications, an unredacted PDF will be shared which may contain the applicant's personal data. This could introduce bias to the process.	1. Leave the personal data on the form (risk of bias) 2. Redact personal data from the form when sharing outside of the named individuals	1. Reduced 2. Eliminated	Low Low	Yes No
An inappropriate person e.g. a child registers with the system in error, or does not go on to make an application.	1. Delete the data if it seems incongruous (risk of losing people who want to apply later) 2. Leave the data until it auto-deletes under the Good Grant system's retention rules	1. Eliminate 2. Reduced	Low Low	No Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Laura Barley 14/03/2023	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Rachel Cook	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Mike Richmond 23/6/2022 & 14/05/2023	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: The risks associated with this processing are very low and the mitigations proposed are, in my opinion, sufficient to minimize any risk to a person's rights and freedoms. I recommend that this DPIA be reviewed in 12 months, or at the point of a change in the process or online system, whichever comes first.		
DPO advice accepted or overruled by:	Rachel Cook	If overruled, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Laura Barley	The DPO should also review ongoing compliance with DPIA

Appendix A - Community Safety Fund & Community Response Fund – Data Processing

Stage	Data Collected	Who has access	Storage	Comments
Application	Project details Organisation details Contact Name, address, email and phone number	• Funding Manager • Funding Officer • Head of Policy and Partnerships • Police & Crime Commissioner	Good Grants system OPCC IT System	No automatic processes involved
Project Appraisal	Application details as above	• Funding Manager • Funding Officer • Head of Policy and Partnerships • Police & Crime Commissioner • Other OPCC team members depending on specialisms	Good Grants system OPCC IT System	Appraisal forms used – no auto processing
Project Approval	Application details as above	• Funding Manager • Funding Officer • Head of Policy and Partnerships • Chief Executive & Monitoring Officer • Police & Crime Commissioner	OPCC IT System	Initially this is an internal decision-making process but external representatives from the Community Safety Partnerships have been consulted.

Decision	Project information not personal data – this will include grant levels and any outputs	Public record	OPCC IT System Published online, PR & Media activities	For the CRF voting rounds will involve the public – this will select the successful project for each location. Applicants are fully aware of this and will not include any personal data.
Formal Offer / Contracting	Application details as above	• Funding Manager • Funding Officer • Head of Policy and Partnerships • Chief Executive & Monitoring Officer • Police & Crime Commissioner	OPCC IT System Good Grants (for future rounds)	
Grant Claims and Monitoring	Application details as above	• Funding Manager • Funding Officer • Head of Policy and Partnerships • Chief Executive & Monitoring Officer • Police & Crime Commissioner • OPCC Finance Team	OPCC IT System	Grant claim process map attached
Evaluation	Application details as above	• Funding Manager • Funding Officer • Head of Policy and Partnerships • Chief Executive & Monitoring Officer • Police & Crime Commissioner	OPCC IT System	