Data Protection Impact Assessment

Title	Step 1: Identify the need for a DPIA	Step 2: Describe the processing				Step 3: Consultation process	Step 4: Assess necessity and proportionality	Step 5: Identify and assess risks		Step 6: Identify measures to reduce risk	Step 7: Sign off and record outcomes					
Start with Reference Number DPCC-XX	*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.*	*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?*	*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?*	*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?*	*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?*	*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?*	*Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.*	*Risk Score*	*Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5*	*Approved by / date*	*DPO Advice Sought?*	*Summary of DPO Advice*	*Consultation Review and Comments*	*Date of next Review*	*Owner*
DPCC-01-Public Surgeries	IA-1 Refers. The PCC offers surgeries so that lessons can be learnt with regard to the way that members of the public are treated by Dorset Police and by the wider criminal justice system. Details provided by members of the public will be, by its very nature, sensitive and may include detail about ongoing criminal cases, convictions, or data that can not be published by law (for example anonymity for Sexual Assault victims). The PCC Surgery Case Worker prepares detailed files to brief the Commissioner and also so that information can be sourced from the Force / other agencies. Should this data be breached, there is potential to cause significant impact on the privacy, wellbeing and safety for victims. There is also the risk, albeit seldom, to cause prejudice to ongoing cases.	The data is collected from members of the public, who provide consent for the data being processed. The data is typically stored in the form of emails, PDF and Word documents on the Network Drive in a protected file. The data is shared with consent, when necessary, with Dorset Police and other relevent agencies.	The data includes personal details, special category (when relevant) - such as ethnicity and disability - and criminal offence data. The cases relate to members of the public throughout Dorset. Volume of data collated is case dependant and can vary. The data is used for the duration of the casework, and again this can vary in duration (usually no longer than 12 months). The data is held on file and may be used again if the individual contacts the OPCC and requests another PCC Surgery.	In some cases, the individuals providing data to the Office of the Police and Crime Commissioner are in contact with the Office on multiple occasions. They are usually members of the public who have been provided with a policing service by Dorset Police- They would reasonably expect the data to be shared both with the Commissioner,Dorset Police and any other involved agency. The member of the public may disclose data relating to children, may be vulnerable or may be offenders or victims. Members of the public are generally concerned about personal data being sold onto other agencies without their knowledge - albeit this is not relevant in this instance.	The PCC hopes to identify areas in which services to members of the public can be improved by either scrutinising the work of the Chief Constable, identifying best practice or multi agency working. The effect on individuals varies - but can assist with closure; rectifiying errors in service provision or receiving formal apologies, for example. The PCC benefits from service improvement; increase in trust and confidence; and demonstration of scrutiny role.	As each PCC Surgery is on a case-by-case basis and consent is required. There is no need for consultation. The processing is all for the purpose as understood by the individual.	The lawful basis for achieving the task is Article 6(1)(a) - consent. The processing helps to achieve positive outcomes for members of the public and there is no obviously apparent alternative.	Loss of Confidentiality: - safety impact; - privacy impact; Loss of Trust and Confidence within Dorset OPCC/Force Prejudice of judicial processes	8	Access control to network path restricted to fewer employees; protective marking on related emails and word documents; retention policy revisited.	Director of Operations 12/7/19 The file has been restricted to five OPCC employees: PCC Surgery Caseworker, PCC, PCCs PA, Head of Policy, Governance & Contact Manager, Protective marking has been added to emails and documents where appropriate. Consent is recorded in the Statement of Understanding document, retained on V drive, in the file of each PCC Surgery case.	Yes - see footnote below re ICO advice in April 2018 and separate Force Legal advice dated 21 February 2019	see footnote below	N/A	Jun-20	Policy Manager

Public Surgeries Footnote: ICO advice to APCC in April 2018 confirmed:

"It will ultimately be for police forces and victim services providers to decide on which lawful basis they will rely on for the processing. It is worth considering other lawful bases apart from consent as the requirements of consent under the new legislation will potentially be difficult to achieve in practice for the reasons set out above.

Moving away from reliance on consent will also mean some of the victim service models could be more straightforward such as where victim services act as a processor on behalf of forces or joint data controller to seek consent from victims before transferring data across to victim services.

It would be helpful if consideration could be given to amending the Code of Practice to clarify the position on consent and to highlight the requirements placed on victim service providers in terms of their role supporting victims.

Lastly, privacy information will need to be very clear whatever the legal bases relied upon as it is important that victims are fully informed in terms of what will happen to their personal data as it moves across the justice system.

Title	Step 1: Identify the need for a DPIA	Step 2: Describe the processing				Step 3: Consultation process	Step 4: Assess necessity and proportionality	Step 5: Identify and assess risks		Step 6: Identify measures to reduce risk	Step 7: Sign off and record outcomes					
DPCC-02-IOPC Referrals	IA-3 Refers. In order that the PCC can scrutinise the work of the Force, the Commissioner needs to be aware of serious reputational matters. For that reason, IOPC referals are passed on by PSD to the OPCC for information. The nature of these documents can be highly sensitive, containing details about crime and victims, as well as personal information.	The data is collected by PSD and passed onto the OPCC. It is only shared with SMT members.	The data includes personal details, special category (when relevant) - such as ethnicity and disibility - and criminal offence data. The cases relate to Dorset Police officers and staff and can include victims. While most referals will relate only to Dorset residents, it is also possible the data refers to those living outside the county.	In most cases, the OPCC would not have a direct relationship with those identified in the referals - although this is not always the case (e.g. a victim may also have asked for a Victim Surgery, see DPCC-01; or been in contact more generally, see DPCC-03). It is not clear whether those identified would expect the data to be shared with the OPCC. However, we know that the public are concerned about various CJS issues - such as death in custody, use of force, and disproportionality - and these referals help the PCC to scrutinise such matters on behalf of the public.	The PCC hopes to identify areas in which services can be improved and also to mitigate the risk of reputational damage to the Force. The effect on individuals is not clear. The PCC benefits from service improvement; increase in trust and confidence; and demonstration of scrutiny role.	It is not certain whether Federation and Unions have been advised of this process. Advice from Legal Services and Information Management has been provided. This confirms that there are a number of lawful bases for processing (see Footnote below in row 10 columns K to R)	The lawful basis for achieving the task is Article 6(1)(e)- Public Task - to hold the Chief Constable to account. The processing helps to achieve positive outcomes for the Force and the only likely alternative is for verbal briefings from PSD / Chief Officers. However, while this does ensure that the information might be shared to fewer people, verbal briefings would likely be inconsistently provided (e.g. not fair) and may suffer from inaccuracy.	Loss of Confidentiality: - safety impact; - privacy impact; Loss of Trust and Confidence within Dorset OPCC/Force Prejudice of judicial processes	8	Access control to network path restricted to fewer employees; protective marking on related emails and word documents; retention policy revisited.	Director of Operations 12/7/19 All files have already been deleted from the Network Drive. The process will now be to forward to SMT for information and no record kept	Yes - see footnote below	see footnote below	N/A	Jun-20	Governance and Contact Manager
DPCC-03-Public Contact	IA-2 Refers. As with any public organisation, the Dorset OPCC receives a great deal of public contact - ranging from invitations, questions about policing and complaints. Details provided by members of the public can, on occasion contain sensitive data and may include detail about ongoing criminal cases, convictions, or data that can not be published by law (for example anonymity for Sexual Assault victims). Should this data be breached, there is potential to cause significant impact on the privacy, wellbeing and safety for victims. There is also the risk, albeit seldom, to cause prejudice to ongoing cases.	The data is collected from members of the public, who provide consent for the data being processed. The data is typically stored in the form of emails and Word documents on the Network Drive. The data is shared, when necessary, with Dorset Police.	The data includes personal details, special category (when relevant) - such as ethnicity and disability - and criminal offence data. The data can relate to anyone - potentially even international - who contacts the office.	The individuals providing data to the Office of the Police and Crime Commissioner can be in contact with the Office on multiple occasions - they are sometimes victims who have been provided with a policing service by Dorset Police. They would reasonably expect the data to be shared both with the Commissioner and Dorset Police. The correspondent may disclose data relating to children and may be vulnerable. Members of the public are generally concerned about personal data being sold onto other agencies without their knowledge - albeit this is not relevant in this instance.	The PCC hopes to identify areas in which services to victims can be improved by either scrutinising the work of the Chief Constable or identifying best practice. The PCC also hopes to provide a useful public service to residents, by assisting with their enquiries. The effect on individuals varies - but can assist with closure; rectifying errors in service provision or receiving formal apologies, for example. The PCC benefits from service improvement; increase in trust and confidence; and demonstration of scrutiny role.	As each public contact is on a case-by-case basis and consent is required there is no need for consultation. The processing is all for the purpose as understood by the individual.	The lawful basis for achieving the task is Article 6(1)(a) - consent. The processing helps to achieve positive outcomes for members of the public and there is no obviously apparent alternative.	Loss of Confidentiality: - safety impact; - privacy impact; Loss of Trust and Confidence within Dorset OPCC/Force Prejudice of judicial processes	6	Access control to network path restricted to fewer employees; protective marking on related emails and word documents; retention policy revisited.		Yes - see footnote below	see footnote below	N/A	Jun-20	Governance and Contact Manager
DPCC-04 Recruitment Files	IA-8 Refers. During the recruitment of volunteers and employees, the Office receives PDF scans of applications (sometimes in full); makes copies of qualifications and ID documents and then subsequently records information through the selection process. This data could include identifying information and personal details, such as ethnicity, disability and sexual orientation, for example.	The data is collected from applicants, who provide consent for the data being processed. The data is typically stored in the form of emails and Word documents on the Network Drive. The data is shared, when necessary, with Dorset Police Recruitment and People Services.	The data includes personal details, special category (when relevant) - such as ethnicity and disability - and criminal offence data. The data can relate to any applicant - potentially even international - who contacts the office.	The information is provided both directly from the applicant and also via the HR Recruitment team. Applicants may be in contact with the OPCC on a number of occasions - naturally successful applicants will be in regular contact with their place of employment. They would reasonably expect the data to be shared both with the Commissioner and Dorset Police. The correspondent may disclose data relating to children and may be vulnerable.	This data is gathered for the purposes of fair and transparent recruitment and, subsequent employment, of staff. The benefits are clear from an individual's point of view (a job) and for the OPCC (staff).	Consultation is not required as this is a routine procedure.	The lawful basis for achieving the task is Article 6(1)(b) - contract; although it could also be argued that there is a lawful basis within 6(1)(a) - consent. The processing helps to ensure fair selection processes and there is no apparent alternative.	Loss of Confidentiality: - safety impact; - privacy impact; Loss of Trust and Confidence within Dorset OPCC/Force	4	Access control to network path restricted to fewer employees; protective marking on related emails and word documents; retention policy revisited.	Director of Operations 12/7/19	Yes - see footnote below	see footnote below	N/A	Jun-20	Governance and Contact Manager

Title	Step 1: Identify the need for a DPIA	Step 2: Describe the processing				Step 3: Consultation process	Step 4: Assess necessity and proportionality	Step 5: Identify and assess risks		Step 6: Identify measures to reduce risk	Step 7: Sign off and record outcomes					
DPCC-05 Personnel Files	IA-8 Refers.	The data is collected from volunteers, who provide consent for the data being processed. The data is typically stored in the form of emails, Word and Excel documents on the Network Drive.	The data includes personal details, special category (when relevant) such as ethnicity and disability - and criminal offence data. The data can relate to any applicant.	The information is provided from the volunteer.	This data is gathered for the purposes of fair and transparent recruitment and, subsequent employment, of staff. The benefits are clear from an individual's point of view (a role) and for the OPCC (staff).	Consultation is not required as this is a routine procedure.	The lawful basis for achieving the task is Article 6(1)(b) - contract; although it could also be argued that there is a lawful basis within 6(1)(a) - consent. The processing helps to ensure fair selection processes and there is no apparent alternative.	Loss of Confidentiality: - safety impact - privacy impact Loss of Trust and Confidence within Dorset OPCC/Force	4	All personnel folders moved to one area and network path restricted to fewer employees, protective marking on related emails and word documents, retention policy revisited.	Director of Operations 12/7/19	Yes - see footnote below	see footnote below	N/A	Jun-20	Governance and Contact Manager

Footnote - Legal Advice

Advice as contained in email from Force Legal dated 21 February 2019:

"There are a number of lawful bases for processing (complete list below for information), and whilst Consent is the preferable option it is not the only one. .

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

I would suggest that given the functions of the OPCC that most disclosures to the Force would be captured by (e) Public Task. In order for the OPCC to carry out its official functions which are in the public interest it would be necessary for the data to be disclosed to the Force.

As discussed the majority of the personal data will be contact information which is necessary in order to identify the person to investigate the complaint or query and to make contact with them when responding. As you noted, the majority of this information is most likely already held by the force in any event.

There may also be cases where legal obligation is applicable depending if in making the disclosure you are complying with legislation, as this does not include contractual obligations, and although I have not read the MOU referred to by Richard Scott, I do not believe it could be relied upon.

As always it would be on a case by case basis, but if the OPCC are satisfied that the disclosure is necessary to either comply with law, it is in the public interest or necessary to carry out their official function then consent will not be required.

I would recommend documenting any decision making and rational where appropriate."