Information Sharing Policy

Author:	*Scrutiny Manager*
Date created:	*July 2019*
Review due/frequency:	*Annual*
Version:	*V0.1*
Current Version Date:	*July 2019*
Approved by Dorset OPCC SMT:	*16 September 2019*

1. Introduction

1.1 The ability to share data between Dorset OPCC and other organisations is crucial in being able to fulfil the Police and Crime Commissioner's statutory responsibilities and deliver the best possible service to the people of Dorset.

1.2 The public must have confidence in the way the OPCC handles their personal data, and that any processing and sharing only takes place where there is a lawful purpose to do so.

1.3 The purpose of this policy is to provide the framework for sharing personal data between the OPCC and other organisations, ensuring the organisation meets the requirements under the General Data Protection Regulation and the Data Protection Act 2018.

1.4 For the purposes of clarity, the term PCC is used to encompass the person elected as the PCC and any staff authorised to work for or on their behalf or under their direction and control (i.e. the Office of the Police and Crime Commissioner or "OPCC").

1.5 The policy takes into account the Data Sharing Code of Practice issued by the Information Commissioner's Office (ICO), although mindful that it has not been updated since the Data Protection Act 2018. Revisions to this policy will be considered upon the publication of any new codes from the ICO.

1.6 This policy should also be read in conjunction with the OPCC's Data Protection Policy.

2 Definition of sharing

2.1 The nature of the work of the OPCC means that sharing information with other organisations takes place on a routine basis. Much of this sharing does not involve personal data, for example where only statistics are shared. This policy does not apply to this kind of sharing.

2.2 There are two types of data sharing covered by this policy:

- *Systematic* – this is routine data sharing where the same data sets are shared between the same organisations for an established purpose; and

- *One-off* – this covers ad hoc decisions to share data which could be for a variety of purposes, which do not fall within agreements made as part of systematic data sharing.

2.3 The two types of data sharing require a different approach, but will both comply with data protection legislation.

2.4 The legislation that governs the work of the OPCC, including the Policing Protocol, requires there to be a close working relationship with Dorset Police, and for information to be exchanged so that both comply with their statutory responsibilities. However, the two organisations are separate data controllers

and are registered with the Information Commissioner's Office as such. As a result, the exchange of information between the two is governed by the same procedures in place for systematic data sharing.

2.5 The ICO Code of Practice focuses on sharing personal data between data controllers, rather than sharing of data between a data controller and any data processors. Where the OPCC as a data controller shares personal information with a data processor, or where a data processor collects and carries out other processing activity on behalf of the OPCC, a formal agreement will be in place that governs the processing activity to ensure it is done in line with legislation.

3 The decision to share personal information

3.1 Personal data should only be shared where there is a clear legal basis to do so, or the data subjects have given their consent. The lawful purposes are set out in the GDPR, with an enhanced level of legal basis required for sensitive personal data as defined by legislation.

3.2 The main legislation that governs the business of the OPCC is the Police Reform and Social Responsibility Act 2011, and associated secondary legislation and regulations.

3.3 Consideration must be given to whether or not an objective or set of objectives can only be achieved by data sharing, or if they can be achieved through other means, such as anonymising the personal data before sharing.

3.4 Before any personal information is shared, a number of data quality checks should also be made:

a) Data formatting – where data is shared with another organisation, consideration should be given to agreeing common data standards to ensure information transfers correctly from OPCC systems into other systems.

b) Data accuracy – ensure there is a sufficient level of reassurance about the accuracy of data has been received. Factors that may affect data accuracy may include age of data, completeness of records, original source, and any ability to cross-reference to other data sets.

c) Data amendments – a procedure needs to be put in place for amending data after it has been shared, if the data recipient is to process this data for an extended period of time.

d) Data retention – where information is not subject to a statutory retention period, the receiving organisation needs to be aware of the OPCC retention policy to ensure organisations do not hold information longer than the OPCC itself, and any requirements to provide assurances around deletion/destruction at the end of the retention period.

e) Data minimisation – ensure consideration has been given to exactly what data is required to achieve the objectives, making sure the minimum amount of personal data is shared.

3.5 Before any systematic or one-off data sharing takes place, it is good practice to consider if a Data Protection Impact Assessment (DPIA) is required. This will help the organisation to assess the benefits of data sharing and balance this against the risks or potential negative effects, both in terms of harm to individuals and to the organisation's reputation. The DPIA tab forms part of the GDPR master spreadsheet which can be found on our shared drive here. In the event of a new DPIA being required an additional row should be added to the spreadsheet in liaison with the Data Protection Officer to refer the proposed new OPCC activity to be assessed from a data protection perspective. (Note: the headings in the spreadsheet reflect the ICO template which can be found here.)

4. The rights of data subjects

4.1 One of the principles of GDPR requires that personal data be processed legally, fairly and transparently.

4.2 The privacy notice on the OPCC website sets out in general terms what personal data is held, how we hold it, what other organisations we share this with, and the legal basis for doing so. It is available here: https://www.dorset.pcc.police.uk/information-hub/publication-scheme/. It is recognised that data sharing arrangements can change over time, and this notice is reviewed regularly to ensure it accurately reflects the activities of the organisation.

4.3 We also choose to inform individuals or groups of organisations through specific privacy notices about how their data is going to be handled, linking to the main privacy notice. This is encouraged:

- where we are sharing sensitive personal data;
- where the data sharing is likely to be unexpected or objectionable;
- where the data sharing will have a significant effect on individuals;
- where sharing is done with organisations that individuals might not expect; or
- where the sharing is being done for a range of different purposes.

4.4 The general rule is that individuals should be aware how their personal data is going to be shared, even if their consent is not needed. However, in certain limited circumstances, the GDPR allows for personal data, even sensitive personal data, to be shared without the individual knowing about it. This can be done where data is processed for the prevention or detection of crime, the

apprehension or prosecution of offenders, or the assessment or collection of tax or duty. While the OPCC is not involved directly in any of these activities, it will co-operate with legitimate enquiries from agencies involved in this work and disclose information in response to lawful orders.

5. Roles and responsibilities

5.1 The responsibility for the sharing of data between the OPCC and other organisations is ultimately with the Chief Executive as the person with delegated authority to carry out all functions and responsibilities of the Data Controller.

5.2 It is however the responsibility of the Senior Management Team (SMT) member who owns individual data sets to ensure that any data sharing is done in accordance with this policy. This responsibility extends to all OPCC staff members, but accountability sits with the SMT member, who is also responsible for signing any Information Sharing Agreements relating to data from their business area.

5.3 The Data Protection Officer will provide advice and support to all OPCC staff to ensure data sharing is carried out in accordance with this policy. They are also responsible for reviewing any Information Sharing Agreement between the OPCC and other organisations.

5.4 The data protection training programme for all OPCC staff will cover the necessary elements of information sharing. This will enable staff to confidently and correctly deal with data sharing matters.

5.5 Where local procedures are written to manage the systematic or one-off transfer of data, references should be made in the associated procedure document to this Data Sharing Policy.

6. Record of data sharing activity

6.1 Where it is determined there will be a large scale sharing of data, or that data sharing will take place on a systematic basis, we will agree a common set of rules to be adopted with the sharing organisation, known as an Information Sharing Agreement (ISA). This agreement will include, but is not limited to, details about the purpose of sharing, the recipients, details of the data, the lawful purpose for sharing, security and retention information, the procedure for dealing with access requests/queries/complaints, and the review period for the agreement.

6.2 The OPCC has an ISA template that sets out the key components of any agreement it will be party to, and forms the basis for discussion with other organisations who may wish to use its own ISA template as the framework for an agreement.

6.3 It is not compulsory that the OPCC enters information sharing agreements using this template. However, the decision to use another organisation's template as the basis for the agreement must be considered by Data Protection Officer to ensure the OPCC is satisfied that all essential components are contained within it.

6.4 The Information Sharing Agreement between Dorset Police and Dorset OPCC is reviewed at least annually. Details of the ISA will be recorded within the IAR. Details of any other Information Sharing Agreement (ISA) will be added to the IAR to maintain a complete record of such ISAs. This record will include dates of agreements to ensure reviews are completed in a timely manner. The relevant information must also be transferred into the Information Asset Register.

6.5 As part of the process to sign off any Information Sharing Agreement, consideration will be given to whether additional fair processing information is appropriate, whether existing privacy notices will need to be updated, or if the current privacy notice will suffice for the additional processing.

7. One-off data sharing requirements

7.1 Where data sharing is done on a one-off basis, a number of conditions will also need to be satisfied before any data sharing takes place. These conditions are not designed to restrict the ability of the organisation to share data with others for genuine business reasons, but respect the legal framework within which it should take place.

7.2 The process flowchart at appendix A should be followed to support the decision-making process, with any decision taken to share data documented in the Data Sharing Activity Log held in the OPCC shared drive here . All stages of the process should be satisfied before any data sharing takes place.

7.3 Personal data should be shared using a secure method of transfer that is proportionate in the circumstances, taking into account what the data is and who it is being shared with. The OPCC must be satisfied that the recipient organisation has appropriate measures against unauthorised or unlawful processing of the data and the accidental loss or destruction of, or damage to the personal data.

7.4 The OPCC will make clear that where there is an actual or potential data incident relating to the personal data supplied, the receiving organisation must report it to the OPCC. The receiving organisation must also co-operate with the investigation into any potential data breach. Details recorded about the breach will be considered should any future data sharing requests be received in the future.

7.5 The provisions placed upon the receiving organisation will be set out in a standard terms document that will accompany any personal data that is released on an ad-hoc basis.

8. Other requirements

8.1 Data sharing does not routinely happen with organisations outside of the European Union. Should any data require transferring to any such organisations, the Data Protection Officer must be consulted to ensure the correct legal mechanism is used to carry out this processing.

8.2 A periodic review process will be introduced to include dip sampling of data sharing requests handled by the OPCC to ensure this policy is being complied with.