Avon and Somerset Constabulary (A&SC)

and the

Police and Crime Commissioner for Avon and Somerset (PCC)

Joint Operating Policy (JOP) – Information Management

1. Purpose:

1.1 The purpose of this document is to provide some guiding principles and to broadly express the inclusive and cooperative nature of the agreed joint approach to the lawful exchange of information between the partner organisations.

1.2 It should be noted that for the purposes of this document the terms *"sharing"*, *"exchanging"* and *"disclosing"* have the same meaning and purpose, as does *"information"* and *"data"*.

2. The need to share information

2.1 The Police Reform and Social Responsibility Act 2011 created the role of PCC; setting out a number of functions to be discharged by that role. In order to discharge those functions there will be a need for information in possession of either organisation to be shared with the other.

2.2 This document does not cover the activities of the PCC with the Police and Crime Panel (PCP) as the Constabulary will not normally be a party to that interaction. It is considered unlikely that the Constabulary will need to share information directly with the PCP.

3. Legal gateway

3.1 Sections 36 and 79 of the Police Reform and Social Responsibility Act 2011 provide the gateway for disclosures. Section 79 places an obligation on the PCC and Chief Officer of Police to have regard to the Policing Protocol in the exercise of their functions. The Policing Protocol is contained within the Statutory Instrument 2011 No. 2744, paragraph 19 which states: *"In order to enable the PCC to exercise the functions of their office effectively, they will need access to information and officers and staff within their Force area. Such access to any information must not be unreasonably withheld or obstructed by the Chief Constable and/or fetter the Chief Constable's direction and control of the Force."*

3.2 The working relationship expressed in the joint vision of the PCC and the Chief Constable[1] is; *"The Commissioner and Chief Constable are committed to establishing and maintaining an open and constructive relationship, built on straight and honest dealing. Everything that we do should be informed by our*

joint vision. Although the Commissioner's primary relationship with the Constabulary is via the Chief Constable she will have cause to communicate regularly with all parts of the organisation. The Constabulary will support the Commissioner in discharging her responsibilities by providing information, arranging access to Districts and Departments and contributing to relevant boards and meetings".

3.3 Where personal or sensitive personal data[2] is disclosed through this partnership by virtue of the Statutory Instrument, the sharing would be considered as being compliant with the Data Protection Act and Human Rights Act. Any further processing must be undertaken in a manner which is also compliant with the requirements of these Acts.

4. Policy oversight

4.1 The disclosure of information will, in the main, be undertaken by individuals from either organisation and they will individually be responsible for ensuring that their actions are in accordance with the terms of this document. However, the general oversight of the operation of the JOP will be undertaken jointly by the following roles on behalf of each organisation;

- Head of Corporate Information Management Department, A&SC
- Office and HR Manager, OPCC

4.2 These post holders will also be responsible for an periodic review of this document to ensure continued relevancy and accuracy in the light of practical working experience and future developments.

5. What information may be shared?

5.1 In principle, where relevant and necessary in order for the office of the PCC to undertake its functions[3], any information held by the Constabulary is potentially able to be shared. This will include both non-personal and personal data.

5.2 Sharing will not take place where there are any specific legal restrictions or where it would fetter, restrict or restrain the Chief Constable's direction and/or control of the Constabulary, or where it may prejudice ongoing or potential investigations and/or prosecutions by the Constabulary or other agency. If information disclosed by the police is designated as being 'not suitable for further dissemination' (for example, information originating from the Security Services) the PCC undertakes to make no further disclosure without the explicit consent of the Chief or Deputy Chief Constable's.

5.3 The PCC will also wish to share data with the Constabulary where it supports a policing purpose[4] or where it is necessary to exercise the functions of the PCC.

6. Process for sharing

6.1 The approach to data sharing will vary depending on the circumstances and it is not the intention of this document to attempt to capture or define those processes. However, it is important that an appropriate level of data integrity is maintained within the mechanism that is considered as the most appropriate at the time of disclosure and also, where reasonable to do so, disclosures of personal data are noted on the original documentation or similar record, to ensure that there is a simple audit trail for reference in any subsequent complaint or litigation.

6.2 Where agents or volunteers are used by either party to process personal data on their behalf the organisation has a responsibility[2] to ensure that these third parties act only within the designated remit of their role and that they treat matters in a manner which preserves the confidence and integrity of the data. The physical means of doing so is a matter for each organisation, for example; a Data Processing Agreement, an undertaking of confidentiality declaration (for reference a template of an undertaking of confidentiality declaration, is attached at appendix 'A') or other similar type of agreement. However, with the exception of the Commissioner, where OPCC staff or their agents/contractors have direct and/or unrestricted access to Police 'owned' personal data and/or IT systems they must be Police Vetted to the appropriate level; including National Security Vetting, where applicable.

6.3 In each case the appropriate level of Police Vetting will be agreed in advance with the Force Vetting Officer. The OPCC will only be expected to pick up costs of vetting if a department of the OCC would be expected to pick up costs for such vetting.

6.4 Should an individual fail to achieve a Vetting clearance the Force Vetting Officer (or Force Vetting Co-ordinator) will advise the OPCC Chief Executive Officer and provide him/her with sufficient information about the reasons for the failure in order that they may undertake an informed and appropriate assessment of the risk of continuing to engage that individual without a clearance. As an independent body, the decision to recruit will always remain that of the OPCC.

6.5 It is acknowledged that in the event of OPCC staff/contractors or Agents failing to achieve an appropriate Vetting clearance but are still required to process Constabulary 'owned' personal data or access Constabulary IT systems for their purposes, the ensuing risk is shared by both Data Controllers. It would normally be expected that persons in that position will be asked by the OPCC to sign a confidentiality agreement (See Appendix A) in order to clarify their position and to help mitigate the risk to all parties. Whilst the Chief Constable reserves the right to refuse access to IT systems and data to persons not holding an appropriate Vetting clearance, it is accepted that in the spirit of openness, cooperation and partnership engagement between the Constabulary and the OPCC that such action would be rarely taken and would only be after consultation between the Chief Constable's Office and the OPCC.

7. Use of information

7.1 Information shared under the terms of this document shall only be used for the purpose(s) for which it was provided, as otherwise required by common or statute law or as subsequently agreed with the relevant Data Controller.

7.2 In addition to any statutory requirements information must be managed and processed securely on a 'need to know' basis and not further disclosed without the agreement of the originating party. In addition, where protectively marked[5] the recipient will undertake to manage the information in accordance with that marking.

7.3 As independent Data Controllers both parties are required to maintain an up-to-date notification[2] to the Information Commissioner and are obliged to ensure that they have appropriate security measures, training, policies and operating procedures in place to enable the effective processing of personal information by their staff and/or third parties acting on their behalf.

7.4 When the information is no longer required it must either be securely returned to the originator or securely destroyed by appropriate means.

8. Complaints

8.1 In the event of a complaint being received about the information exchanged or the manner in which it has been used by the other organisation, the receiving party will advise the other party as soon as possible and in any event before responding to the complaint.

8.2 It is anticipated that both organisations will, where appropriate, work together to resolve complaints, however it is worth noting that as independent Data Controllers[2] each organisation retains responsibility and liability for its processing of personal data.

9. Requests for information under the Data Protection and Freedom of Information Acts

9.1 It is essential that both organisations work closely together to manage requests for information that may originate from or impact on the operations of the other party. Whilst both organisations fully embrace the transparency agenda it is recognised that there are occasions where the application of exemptions are both necessary and appropriate in the greater public interest; for example, to protect the integrity of operational policing.

9.2 **Data Protection Act (Subject Access).** All requests for information under the Subject Access provisions of the Data Protection Act 1998 will be dealt with by the person responsible for Data Protection within the organisation. If personal data is identified as belonging to the other party, it will be the

responsibility of the receiving party to contact the Data Protection Officer for the originating party to determine whether the latter wishes to claim an exemption under the provisions of the Data Protection Act.

9.3 **Freedom of Information Act.** Requests for personal information by the data subject under the Freedom of Information Act will be dealt with under the amended 'Subject Access' provisions of the Data Protection Act. Where a request is received for non personal data or for third party personal data which has originated from the other party, the recipient should liaise with the 'owning' party before disclosing to ensure that there is no wish to claim an exemption under the Act.

10. Signatories

10.1 By signing this Joint Operating Policy the Police and Crime Commissioner and the Chief Constable acknowledge the requirements placed upon them when sharing information in support of the legitimate activities of either or both organisations.

Signed on behalf of Avon and Somerset Constabulary

By ..... On 04/08/2017

Name, title and position ACC Sarah Crew

Signed on behalf of the Police and Crime Commissioner

By ..... On 4/8/17

Name, title and position OPCC-CEO

Notes:
[1] Extract from the "Joint Vision Avon and Somerset Police and Crime Commissioner and Chief Constable", dated 4th March 2013
[2] As defined by or required under the Data Protection Act 1998
[3] As defined under the Policing Protocol Order 2011
[4] As defined by the Management of Police Information, Statutory Code
[5] As defined by the Government Security Classification or future equivalent scheme

Appendix 'A'

Undertaking of Confidentiality

I [name of individual] as a [insert role] working with the [insert Avon and Somerset Constabulary or Police and Crime Commissioner of Avon and Somerset] involved in [insert details of specified activity] hereby acknowledge the responsibilities arising from this activity.

I understand that my part in fulfilling this activity means that I may have access to police data (personal and non-personal data) and that such access may include, but not limited to:

- reading or viewing of information held on computer or displayed by some other electronic means,
- reading or viewing manually held information in written, printed or photographic form, or
- overhearing or being a party to any radio, telephone or verbal communication.

I undertake that;-

- I shall not communicate to nor discuss with any other person the contents of this data except to those persons authorised by the Data Controller as is necessary to progress the agreed Purpose.
- I shall not retain, extract, copy or in any way use any data to which I have been afforded access during the course of my role for any other purpose.
- I will only operate computer applications or manual systems that I have been trained to use and will only use them for the purposes for which I am intended to do so. This training will include the requirements of the Data Protection Act 1998 which prescribes the way in which personal data may be obtained, stored and processed.
- I will comply with the appropriate physical and system security procedures made known to me by the Data Controller.
- I will act only under instruction from the [add details of postholder] or other relevant official in the processing of any data.

I understand that all personal data is subject to the provisions of the Data Protection Act 1998 and that by knowingly or recklessly acting outside the scope of my role or any specific instructions given to me, I may incur criminal (e.g. Official Secrets Act, Data Protection Act and Computer Misuse Act) and/or civil liabilities arising from any form of misuse or breach.

I undertake to seek advice and guidance from the [add details of postholder] or other relevant official in the event that I have any doubts or concerns about my responsibilities or the authorised use of the data to which I am afforded access

I understand and undertake that I will treat all information as confidential and that the need to do so shall survive termination of this activity.

I have read, understood and accept the above.

Signed:

Name:

Date: