AVON AND SOMERSET CONSTABULARY ("THE CONSTABULARY")
AND
THE POLICE AND CRIME COMMISSIONER FOR AVON AND SOMERSET ("PCC")

INFORMATION SHARING AGREEMENT

Purpose

1. The purpose of this document is to set out the terms and conditions under which information held by the Constabulary will be lawfully shared with the PCC (and PCC's office) and vice versa.

2. This agreement recognises that effective joint working is vital in the prevention and detection of crime, support to victims and witnesses and meeting the expectations of the public.

3. This agreement has been developed with reference to the Data Protection Act 2018, the General Data Protection Regulation, the Police Reform and Social Responsibility Act 2011 and the Policing Protocol 2011.

The need to share information

4. The PCC is required by law to hold the Chief Constable to account for the effective and efficient policing by the Constabulary.

5. The PCC is specifically tasked to:

   5.1 Secure the maintenance of the Constabulary.

   5.2 Secure that the Constabulary is efficient and effective.

   5.3 Hold the Chief Constable to account for the performance of the Constabulary and for the exercise of the functions under the direction and control of the Chief Constable.

   5.4 Set the Police budget, the police share of Council tax and the local 'Police and Crime Plan' which sets out the overall strategy for Policing in the Constabulary area.

   5.5 Monitor and take a role in Police Complaints.

6. In order to successfully fulfil these functions, the PCC will need to be supplied by the Constabulary with relevant information about policing matters. The PCC will receive complaints and enquiries about policing matters and other matters within the role of the PCC that will require liaison with the Chief Constable and Constabulary Officers/Staff and sharing of information to ensure public confidence and the best service to the public.

Legal gateway

7. Section 36 of the Police Reform and Social Responsibility Act 2011 requires that the Chief Officer of Police must give the PCC such reports on policing matters that the PCC may require the Chief Officer to give. The Act also states that such information must be in a form (if any) specified by the PCC (the elected local policing body). The Policing Protocol provides that:

   "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."

8. Where information is shared between the parties to this Agreement any transfer of information must be compliant with the Data Protection legislation and the Human Rights Act, as must any further processing of that information by either party.

Policy oversight

9. 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 and the relevant legislation.

10. However, in addition, general oversight of the operation of this Agreement and the sharing of information pursuant to it will be undertaken jointly by the following roles on behalf of each organisation:

    Joint Data Protection Officer – Constabulary
    Chief Executive Officer – PCC's office

11. They will also be responsible for periodic reviews of this document to ensure continued relevancy and accuracy in the light of practical working experience and future developments.

What information may be shared?

12. Information that is relevant and necessary in order for the PCC to undertake the functions defined in the Policing Protocol Order is potentially able to be shared. This will include both non-personal and personal data.

13. 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.

14. The PCC will also wish to share data with the Constabulary where it supports a policing purpose or where it is necessary to carry out the functions of the PCC.

Process for sharing

15. The following principles should be applied when sharing information between the Constabulary and the PCC:

15.1 The default will be to share all information required for the PCC to carry out the PCC's functions in an open and transparent way.

15.2 Information requests will not interfere with operational policing e.g. there should be no need to request information about individual Offenders or Victims, unless of high profile or public concern.

15.3 Information requests will be proportionate, for a clearly defined purpose and will not place an unreasonable administrative burden on either party in this agreement.

15.4 Data shall be shared using secure systems and when no longer required shall be disposed of securely. This includes but is not limited to: retention periods, breach policies, training policies and privacy impact assessments.

15.5 The Constabulary and the PCC will work together to resolve any differences and find an appropriate way forward for working together.

15.6 Personal data will be shared when it is the only effective way to allow the parties to fulfil their respective roles.

15.7 The parties will make the data available after it is shared only to those who need to have it to carry out their functions.

15.8 Special category data may also be shared pursuant to this agreement but usual additional consideration as to the need to share it in order to allow the parties to fulfil their statutory obligations will be given.

15.9 The PCC will observe the requirement of the Constabulary with regard to vetting and physical security of officers, systems and offices where data is shared.

15.10 Disclosure of personal data should be recorded in order to ensure that there is a simple audit trail for reference in any subsequent complaint or litigation.

15.11 Where agents or volunteers are used by either party to process personal data on their behalf the organisation has a responsibility 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.

Use of information

16 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 between the relevant Data Controllers.

17 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 the recipient will undertake to manage the information in accordance with that marking.

18 As independent Data Controllers both parties are required to maintain an up-to-date notification 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. The ISO/IEC 27002:2013 Code of Practice for Information Security Management provides a baseline for security arrangements.

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

Complaints and liability for breaches

20 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.

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

22 Each party will be accountable for any misuse of the information supplied to it and the consequences of such misuse by its employees, servants, or agents.

23 Breaches and any immediate action taken to mitigate the risk caused by that breach must be notified to the originating partner as soon as is practicable, and in any case, within 72 hours. Consideration should also be given as to whether there is an obligation to notify the Information Commissioner's Office (ICO) of any breach – information as to when the duty to notify arises can be found on the ICO website.

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

24 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 transparency 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. ***Data Protection Act (Subject Access)*** - All requests for information under the Subject Access provisions of the GDPR 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 other party for the originating party to determine whether the latter wishes to claim an exemption under the provisions of the GDPR.

25 ***Freedom of Information Act*** - Requests for information by the data subject under the Freedom of Information Act will be dealt with under the amended 'Subject Access' provisions of the GDPR. 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.

Signatories

26 By signing this Information Sharing Agreement 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 24/12/18

Name, title and position Chief Constable Andy Marsh

Signed on behalf of the Police and Crime Commissioner for Avon and Somerset

By ..... On 21/12/18

Name, title and position Sue Mountstevens, Police & Crime Commissioner for Avon & Somerset.