DONNA JONES

POLICE & CRIME COMMISSIONER

HAMPSHIRE & ISLE OF WIGHT

Information Sharing Agreement

Summary:	An agreement to formalise the information sharing arrangements necessary to enable the Police and Crime Commissioner to carry out their statutory functions
Parties to the agreement:	Police and Crime Commissioner for Hampshire & Isle of Wight Hampshire & Isle of Wight Constabulary
Review period:	Annual
Agreement owner:	Police and Crime Commissioner for Hampshire
Agreement drawn up by:	Police and Crime Commissioner for Hampshire
Reviewed by:	Hampshire & Isle of Wight Constabulary – Joint Information Management Unit
Version:	V5 03/02/2025

1. Introduction

1.1 This Information Sharing Agreement (ISA) has been developed between the Chief Constable of Hampshire & Isle of Wight Constabulary and the Police and Crime Commissioner of Hampshire & Isle of Wight (the 'PCC') to explain:
- why the parties have agreed to share information;
- the legal justification behind the sharing;
- who, on behalf of each party, has managerial oversight and responsibility for the information sharing;
- the principles by which information will be shared and used;
- how miscellaneous matters will be managed.

1.2 For the purposes of this ISA, the term "sharing" information means providing or disclosing information to the other party by appropriate means.

1.3 For the purposes of this ISA, 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").

1.4 For the purposes of this ISA, the term Chief Constable is used to encompass the occupant of the Office of Chief Constable and any officer or staff members under their direction and control (i.e. Hampshire Constabulary).

2. Objectives and purpose of the Information sharing

2.1 The Police Reform and Social Responsibility Act 2011 created the role of PCCs for policing areas in England and Wales and set out the functions that the PCCs must discharge.

2.2 In order for the PCC to discharge those functions, there is a requirement for information in the possession of the Chief Constable to be shared with the PCC. A specific, reciprocal sharing of information from the PCC to the Chief Constable may also be required to assist in the discharge of the PCC's or the Chief Constable's functions or for policing purposes.

2.3 The Police (Complaints and Misconduct) Regulations 2020 introduced a statutory duty for the PCC within the police complaints system and set out the functions that the PCC must discharge. There is a requirement for information to be shared between the two parties to fulfil the PCC's and the Chief Constable's statutory functions.

2.4 The parties to this agreement (the Partner Organisations) agree that information shared under this arrangement between the PCC and the Chief Constable will only be used for the purposes set out in this agreement and will not be used for any other purpose including commercial or marketing purposes.

3. What data will be shared and how long will it be kept?

3.1 The Police and Crime Commissioner to the Chief Constable of Hampshire & Isle of Wight Constabulary

a) Staff and volunteer personnel information, for functional HR and IT purposes;
b) Suppliers contact information, for the processing of payment information;
c) Correspondence from members of the public relating to operational policing matters;
d) Correspondence from members of the public relating to complaints and review applications against Hampshire & Isle of Wight Constabulary through the PCC's role as appropriate authority and local policing body;
e) Estates and Facilities Management information, including service level agreements and compliance;
f) Other Information requests, including public survey reports, commissioning documentation and performance reports.

3.1.1 The data will be securely stored and disposed of in accordance with the Chief Constable of Hampshire & Isle of Wight Constabulary's data retention policy.

3.2 The Chief Constable of Hampshire & Isle of Wight Constabulary to the Police and Crime Commissioner

a) Custody records to enable the PCC to perform the functions of the Independent Custody Visiting scheme (subject to detainee's consent) to verify detainee entitlements under PACE are given, medical/dietary needs met, assessment of risk/vulnerability, the timings of reviews and cell inspections;
b) Details of complaints against the force, its officers and staff to enable the PCC to exercise their statutory oversight, scrutiny function relating to the police complaints system and to exercise their statutory role as the local policing body and appropriate authority within the police complaints system, access to Centurion provides the main data source and access to Dems360 to review body worn video footage as referred to in complaints;
c) Correspondence from members of the public to enable the PCC to exercise their statutory oversight and scrutiny function relating to efficient and effective policing;
d) Work locations of officers and staff for estate management purposes;
e) Details of reasonable adjustments required by individual officers and staff by location for estate management purposes (which could include special category data);
f) Identified members of the OPCC Performance and Delivery Team to be given direct access to all force power-bi dashboards to enable the PCC to exercise their statutory oversight and scrutiny function relating to efficient and effective policing. The OPCC staff will not access personal data behind the force power-bi dashboards
g) The PCC staff have direct access to Hampshire & Isle of Wight Constabulary data via Business Objects which supports the PCC in exercising their statutory oversight and scrutiny function relating to efficient and effective policing

h) Specific PCC staff members will only be granted access to Hampshire & Isle of Wight Constabulary's Record Management System (RMS) for the purposes of fulfilling the following specified activities in relation to the statutory functions of their role:

- To identify any risks to the Commissioner and her staff when attending face to face public meetings.
- To improve the OPCC's service when managing the Commissioner's correspondence and casework: 1) to understand the operational position of the force on the matter raised and to hold the force to account in providing an effective police response to individual matters, 2) support a coordinated response to persistent callers/complainants.

This does not mean that RMS is a guaranteed right and other methods of information provision should always take primacy if more proportionate than direct access. This includes where existing RMS access is required for a new specified activity, where Hampshire & Isle of Wight Constabulary will need to assess the most proportionate provision of information for the new activity.
i) Case files for the Out of Court Disposals Board.
j) Specific information and reports that are shared with the PCC on either a weekly, monthly or quarterly basis to enable the PCC to exercise their statutory oversight and scrutiny function, including Gold Summary and Corporate Communications documents, Force Performance Group slide decks and reports, Uplift Trackers and HR Reports, Organisational Risk Registers and Finance Reports, and Hot Topics Briefings and PSD Briefings (misconduct matters). This information may contain identifiable personal data.
k) A member of PCC staff will be provided with a bespoke anonymised dashboard on the GovMetric Victim Satisfaction Survey (VSS) platform, which is used to manage survey responses from victims. They will also be provided with an anonymised data extract for the Domestic Abuse surveys.
l) The OPCC has a statutory duty to appoint panel members for gross misconduct hearings and police appeals tribunals, therefore, during the course of these arrangements, are provided with the names of officers under investigation for misconduct.
m) Any new initiatives led by the OPCC, requiring access to information, will be considered separately through a bespoke information governance process and only added to this Information Sharing Agreement at the next review if the specific sharing of information is established as business as usual.

3.2.1 The data will be stored and disposed of in accordance with the PCC's Record Retention and Disposal Policy.

3.3 The above data sets are those that are shared on a regular basis. Both Partner Organisations recognise that there will be occasional, ad hoc and sometimes urgent requests for exchanges information. These requests are often sensitive, time critical and may contain personal data and, where this takes place, the Partner Organisation that is the controller of the data must ensure there is a lawful basis for the processing to take place, and follow the procedure set out in its Data Sharing Policy and this Information Sharing Agreement.

3.4 Whilst both Partner Organisations are committed to sharing the information required to carry out their respective public functions, it is recognised that some documents may include sensitive information that is not necessary to share. Such information may be redacted to enable the remaining document to be shared.

4. Data Controller

4.1 Whilst each Partner Organisation will be the data controller for the original version of the information that has been shared, the Partner Organisation that receives a copy of the shared information will become the data controller of that shared copy. Data controller has the meaning as defined by the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018) (and any successor legislation) for the personal data it holds and retain the responsibilities held with this position. It is understood by both organisations that the sharing takes place with some agreed and accepted limitations such as: authorisation must be obtained from the sharing organisation if the receiving organisation wishes to share the received information outside of their organisation or use it for a different purpose than it was original shared for.

4.2 Each Partner Organisation confirms that it is registered with the Information Commissioner's Office as a Data Controller.

4.3 Each Partner Organisation will ensure that any personal data received under this agreement will only be used for the purposes defined in this agreement.

4.4 Each Partner Organisation as a Data Controller acknowledges its obligations under the GDPR and DPA 2018 when processing personal data, which can include collecting, storing, amending and disclosing data.

4.5 Each Partner Organisation agrees that they will only process personal data shared under this agreement within the EU. Should they wish to process personal data outside the EU they will obtain the prior written consent from the signatory of the Partner Organisation.

5. Arrangements for the safe transmission of data

5.1 The personal data shared between the Partner Organisations will be shared using secure methods of transfer.

5.2 The primary methods will be via standard corporate email, which is appropriately secure up to OFFICIAL-SENSITIVE, or by MS Teams/SharePoint file sharing. Both Partner Organisations use the same IT network.

5.3 Due to both Partner Organisations using the same IT network, it is possible for personal data to be obtained directly from software applications, with PCC staff provided with individual login details and accounts for this purpose. This

negates the need to remove personal data from secure applications and transferring it via email. Safeguards in place to protect against the misuse of access include routine system audit capabilities, limited access to approved staff and the requirement of OPCC staff to be vetted and to complete training mandated by the Constabulary.

5.4 Where personal data is required to be transferred in hard copy format, this will be done using the internal courier system as per the requirements set out here: http://www3.hants.gov.uk/htm/htm-courier/htm-confidential-mail.htm.

5.5 Once the personal data is shared between the Partner Organisations it will be necessary for it to be stored securely to ensure that it is protected and is not easily accessible. All approved officers within the Partner Organisations must ensure that they take appropriate measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data. These measures must include saving documents on police network computers in buildings that have police access control systems.

6. Legal Justification for Sharing the Data

6.1 The lawful basis for processing personal data will depend on the particular case. In most cases it is likely to be necessary to carry out a 'public task' e.g. under the Police Reform and Social Responsibility Act 2011 and Police Reform Act 2002 and Police (Complaints and Misconduct) Regulations 2020. On occasion it will be necessary to process criminal offence data for reasons of substantial public interest. Explicit consent will also be a lawful purpose, particularly in cases where correspondence/complaints contain special category data.

6.2 The legal justification for the sharing of information between the parties is derived from the Police Reform and Social Responsibility Act 2011 ("the Act") and the "Policing Protocol" (SI 2011/2744). According to paragraph 19 of the Policing Protocol:

"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."

6.3 Personal data may only be shared where there is a specific lawful purpose under Article 6 GDPR and Article 9 GDPR (when the sharing includes Special Category Data). The basis for use of Article 6 information will vary depending on the particular circumstance, but will include contract, public task, legal obligation and consent. For Article 9 data, the basis for sharing will include consent, vital interests of the data subject and the establishment, exercise or defence of legal claims.

6.4 It is accepted and agreed by both parties that it may be necessary to share information in order to enable the PCC to discharge his/her statutory functions and/or for a policing purpose.

6.5 Each Partner Organisation will record the processing of individual personal data sets in its Information Asset Register and make it available for viewing on request to each other.

7. Fair Processing/Privacy Notices

7.1 The Partner Organisations to this agreement recognise their duty under the GDPR to provide information proactively and on request to individuals about how their information is processed.

7.2 Each Partner Organisation will ensure that their privacy notices give details of the processing of personal data and will be provided when:

- the data is collected from a data subject; or
- they receive personal data from another organisation.

7.3 The sharing of information under this agreement is covered by the following privacy notice(s) published by the Partner Organisations to this agreement:

- https://www.hampshire.police.uk/privacy/
- https://www.hampshire-pcc.gov.uk/privacy-policy

8. Responsibilities when Sharing Information

8.1 Each Partner Organisation shall be responsible for ensuring that they have technical, organisational and security measures in place to protect the personal data and to ensure the lawful use of such information shared under this Agreement.

8.2 Each Partner Organisation accepts responsibility for independently or jointly auditing compliance.

8.3 Each Partner Organisation shall ensure that their staff comply with their rules and policies in relation to the protection and use of shared data and that staff have received sufficient training and are aware of their individual responsibilities in relation to data protection and the confidentiality, integrity and availability of personal data. Each organisation will ensure that appropriate sanctions and disciplinary procedures are in place to deal with non-compliance.

8.4 Each Partner Organisation shall have a written policy for the retention and disposal of the personal data shared under this Agreement. As stipulated at sections 3.1.1 and 3.2.1 of this agreement.

8.5 Each Partner Organisation shall be aware that consent should only be relied on as the basis for processing and sharing the data where there are no other

legal basis under the GDPR. Partners shall be aware that a data subject may withdraw consent at any time to the processing of their personal data and therefore further processing must cease.

8.6 Staff of either Partner Organisation may only be permitted access to the personal data shared under this Agreement when necessary in order for them to perform their duties in connection with the services they are required to deliver.

8.7 This Agreement does not permit unrestricted access to the personal information held by the other Partner Organisation. It sets out the parameters for the safe and secure sharing of information for a justifiable need to know purpose, linked to the statutory functions of each organisation.

8.8 Each Partner Organisation shall be responsible for ensuring every member of its staff with access to the personal data shared under this Agreement is aware of and complies with their obligation under the GDPR, DPA 2018, their common law duty of confidentiality and the responsibility to disclose information only to those who have a right to see it. The mandatory e-learning package issued for completion by Constabulary employees is also required to be completed by OPCC employees.

8.9 Each Partner Organisation shall ensure that any of its staff accessing information follow the principles and standards that have been agreed and incorporated within this Agreement.

9. Restrictions on use of Information Shared

9.1 All information must only be used for the purpose(s) specified in this agreement unless required under statute or regulation, or by court order.

10. Security

10.1 The Partner Organisations shall have appropriate technical and organisational measures in place to protect the security, confidentiality, integrity and availability of the personal information (both electronic and hard copy) during all stages of processing (e.g. transfer, storage, access and deletion). This is outlined in section 5.

10.2 Each Partner Organisation shall advise each other should there be any significant changes to the processing of personal data (e.g. transfer, storage, access and deletion).

11. Training

11.1 All Partner Organisations will ensure that any staff processing information shared under this Agreement are trained in data protection and are fully aware of their responsibilities to maintain the accuracy, security and confidentiality of personal information in an efficient and lawful manner. Staff will also be made aware of the requirements to provide privacy notices when sharing or receiving personal data.

11.2 To ensure a common level of understanding, staff of both Partner Organisations must complete the Managing Information NCALT e-learning package.

12. Individual Responsibilities

12.1 Every individual working for the Partner Organisations is responsible for the safekeeping of any information they obtain, handle, use and disclose.

12.2 Individuals with direct access to police systems will only use those systems in order to fulfil a specified statutory activity / function.

12.3 Every individual should know how to obtain, use and share information they legitimately need to do their job.

12.4 Every individual should follow the guidelines set out in this Agreement and seek advice when necessary.

13. Data Accuracy, Rectification, Erasure and Portability

13.1 Each Partner Organisation will ensure that the personal data they process and share under this agreement is accurate and up to date.

13.2 Each Partner Organisation shall inform the other of any rectification or erasure of personal data or restriction of processing as required under Article 19 GDPR.

14. Subject Access Requests

14.1 Every individual has a right under Article 15 of the General Data Protection Regulations to request their personal data.

14.2 Each Partner Organisation will process Subject Access Requests for the information it holds in line with their existing policies and practices, redirecting requestors under existing procedures, when the request is for data not held by that Partner Organisation.

14.3 For the avoidance of doubt personal information supplied by the Partner Organisation will be treated as third party and will therefore require the permission of the other Partner Organisation for it to be released.

15. Data Protection Incidents

15.1 On becoming aware of a potential data breach regarding the data identified in section 3.1, the Chief Constable of Hampshire & Isle of Wight Constabulary's named contact will alert the Police and Crime Commissioner's Data Protection Officer at opcc.dataprotection@hampshire.pnn.police.uk within 24 hours.

15.2 On becoming aware of a potential data breach regarding the data identified in section 3.2, the Police and Crime Commissioner will alert the Chief Constable of Hampshire & Isle of Wight Constabulary's via the ICT self-service portal data breach reporting form within 24 hours (https://tvphcprd.service-now.com/sp?id=sc_cat_item&sys_id=0bfbfbd2dbf937001e48fba668961985&sysparm_category=462702b5dbb973001e48fba66896192e).

15.3 The Partner Organisations will co-operate with each other in the investigation of any potential data breach. Any notification to the Information Commissioner's Office will be completed by the Partner Organisation that is the controller of the data at the centre of the incident.

15.4 The Partner Organisations will ensure that they implement any changes to processes or procedures required as a result of a data incident.

16. Commencement of this Agreement:

16.1 Data will be shared under this Agreement between the Police and Crime Commissioner and the Chief Constable of Hampshire & Isle of Wight Constabulary from the date when a named individual of each organisation signs the Declaration of Acceptance and Participation (below).

17. Review Arrangements

17.1 This Agreement will be reviewed annually and amended only where necessary.

17.2 Any of the signatories can request an extraordinary review at any time where a joint discussion or decision is necessary to address developments or issues.

DECLARATION OF ACCEPTANCE AND PARTICIPATION

(All sections of this form must be completed)

We the undersigned agree that each Partner Organisation that we represent will adopt and adhere to this Information Sharing Agreement:

Chief Constable of Hampshire & Isle of Wight Constabulary

Your Name:	S ARLETON
Your Position:	CHIEF CONSTABLE
Signature:	
Date:	3/2/25

Name(s) and email address(es) of individual(s) acting as main contact(s):	

The Police and Crime Commissioner

Your Name:	Donna Jones
Your Position:	Police & Crime Commissioner
Signature:	
Date:	3rd Feb 2025

Names and email addresses of individuals acting as main contacts:	