

INFORMATION SHARING AGREEMENT



POTENTIALLY DANGEROUS PEOPLE (PDP) - INFORMATION SHARING AGREEMENT (ISA)

BETWEEN

Hampshire Constabulary

AND

**Named Agencies in Section 1 and Appendix B
Version 2.0**

Date Agreement comes into force:	21/12/2018
---	------------

1. INTRODUCTION 2

2. PURPOSE 3

3. STATUTORY POWERS TO PROCESS PERSONAL DATA 3

4. PROCESS 4

4.1 *THE AGREEMENT 5*

4.2 *HOW / WHAT INFORMATION WILL BE SHARED 5*

4.3 *CONSTRAINTS ON THE USE OF INFORMATION 6*

4.4 *RESTRICTIONS ON INFORMATION SUPPLIED 6*

4.5 *REVIEW OF THE INFORMATION SHARING AGREEMENT 6*

5. BREACHES 7

6. SIGNATURES 7

APPENDIX A: GOLDEN RULES FOR INFORMATION SHARING 8

1. INTRODUCTION

- i. Hampshire Constabulary are committed to tackling Crime and Disorder across Hampshire and work, on a regular basis, with members of:
 - National Probation Service
 - Southern Health NHS Foundation Trust
 - Aurora New Dawn
 - Portsmouth City Council (Housing)
 - Southampton City Council – Pathways, No Limits, Inclusion & Virtual School
 - Hampton Trust
 - Up2U
 - Catch 22
 - Circles
 - Child and Adolescent Mental Health Services (CAMHS)
 - Mildmay Oaks Low Secure MH Facility (Priory Group)
 - Winchester Cathedral Safeguarding
 - Sentinel Housing Key 2 Housing
 - IOW Council
 - IOW NHS Primary Care Trust
 - IRIS – Island Recovery Integrated Services (Drug and Alcohol)
 - Any other agency required to attend the PDP meeting

This is in order to make Hampshire safer and provides a framework for action.

The purpose of this agreement is to formalise the information sharing arrangements for the purpose of specific Information sharing pursuant to Crime and Disorder reduction through partnership working.

A potentially dangerous person (PDP) is a person who has not been convicted of, or cautioned for, any offence that places them into one of the three Multi Agency Public Protection Arrangements (MAPPA) categories but whose behaviour gives reasonable grounds for believing that there is a present likelihood of them committing an offence that will cause serious harm.

The decision to nominate an individual as a PDP should be taken in consultation with any other relevant agencies that may currently have, or previously have had, dealings with that nominal. This will result in a meeting between Hampshire Police and other relevant agencies. The decision taken has to be approved by the Police Superintendent within the business area responsible for Public Protection.

A meeting could take place at any time through the year. Due to the nature of the meeting it is unfeasible to name all agencies that may be required to attend. This Information Sharing Agreement (ISA) enables the Data Controller to add agencies when needed.

- ii. This agreement should also be used to further clarify any current arrangements.
- iii. The disclosures originating from this Agreement will comply with The General Data Protection Regulations (GDPR) (2016/679), the Data Protection Act 2018 and all applicable laws and regulations relating to the processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner's Office. The schedules form part of this agreement and shall have effect as if set out in full in the body of this agreement.

2. PURPOSE

- i. This agreement sets out the framework for the sharing of personal data between the parties. It defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other.
- ii. This agreement is in place to inform the reasons and methods of sharing, sharing for other purposes and other information is not covered by this agreement.
- iii. The purpose of this agreement is to enable action to be taken against crime and anti-social behaviour within the local authority area. It will incorporate measures aimed at:
 - Facilitating a coordinated approach that targets crime and anti-social behaviour.
 - Facilitating the collection and exchange of relevant information.
- iv. This agreement is in place to inform the reasons and methods of sharing, sharing for other purposes and other information is not covered by this agreement.
- v. Data can only be used for the purpose shared and cannot be shared to third parties without written permission. Information that may prejudice an ongoing investigation will not be shared unless there is an overriding safety requirement.

3. STATUTORY POWERS TO PROCESS PERSONAL DATA

- i. The principle legislative instruments that provide powers to lawfully share information under this agreement are:
- ii. **The Human Rights Act 1998:** Hampshire Constabulary (HC) as a public authority is duty bound to act in compliance with the Act. Article 8 states that everyone has a right to respect for his private and family life, home and correspondence by a public authority. Interference of this right by HC is not in contravention of the Act if it is in accordance with the law and is necessary, justified and proportionate in a democratic society in the interests of:
 - Public Safety;
 - National Security;
 - Prevention of crime and disorder;
 - Protecting the rights and freedoms of others.
- iii. **Code of Practice on the Management of Police Information (MoPI) 2005:**
4.8. Sharing of police information outside the UK police service:

“Chief Officers may arrange for other persons or bodies within the UK or overseas to receive police information where the chief officer is satisfied that it is reasonable and lawful to do so for the purposes set out at Section 2.2.2. In deciding what is reasonable, chief officers must have regard to any guidance issued under this Code.”

For the purposes of this Code, police purposes are:

- Protecting life and property,
- Preserving order,
- Preventing the commission of offences,
- Bringing offenders to justice, and
- Any duty or responsibility of the police arising from common or statute law.

- iv. There are other pieces of legislation that place powers or duties to share information on public authorities – this list is not meant to be exhaustive. All information sharing must be conducted in accordance with one or more of the legal powers / duties.
- v. Each party shall ensure that it processes the Shared Personal Data fairly and lawfully and ensure that it processes the Shared Personal Data on the basis of a lawful basis.

- vi. **Sharing personal data for the Law Enforcement Purpose** (under Part 3 of the Data Protection Act 2018):

Where the sharing of personal data is between the Hampshire Constabulary and other Competent Authorities (as defined by Schedule 7 of the Data Protection Act 2018) for any of the Law Enforcement purposes (prevention / investigation / detection / prosecution of criminal offences, execution of criminal penalties, safeguarding against and preventing threats to public security) the following lawful basis applies for the processing of special categories of personal data:

- A function conferred by enactment or rule of law, necessary in the substantial public interest

- vii. **Sharing personal data under the General Data Protection Regulation** (under Part 2 of the Data Protection Act 2018):

Where the sharing of personal data is between the Hampshire Constabulary and other Non-Competent Authorities; or the sharing is for a non-Law Enforcement Purpose, the following lawful bases apply for the processing of personal data:

Personal Data:

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the parties.

Special categories of personal data and for non-Competent Authorities to process criminal data:

- Preventing/detecting unlawful acts.

4. PROCESS

This agreement has been formulated to facilitate the exchange of information between partners. It is, however, incumbent on all partners to recognise that any information shared must be justified on the merits of each case. The objective of information sharing in relation to PDPs is to identify risk to the public, criminal behaviour of the subject, opportunities to reduce risk and prevent further criminal offences from being committed, joint agency intervention options, safeguarding of vulnerable people and to formulate an effective risk management plan to reduce and minimise risk.

A PDP referral can be submitted to the Police internally or by a partner agency. This will be reviewed by a Detective Sergeant within the Offender Management Hub. If the referral meets the criteria for PDP status then this will be further reviewed by the Hub Detective Inspector. If agreed then the referral is forwarded to the Detective Superintendent for Public Protection who will ratify the decision or decline.

If the Detective Superintendent agrees that the subject is suitable to be managed as a PDP then a multi-agency meeting will be coordinated which will involve relevant agencies who can contribute

information to develop a risk management plan. This PDP meeting will be chaired by the respective Area Offender Management Detective Inspector.

4.1 THE AGREEMENT

- i. This ISA applies to any personal or confidential information, irrespective of the medium in which it is held e.g. paper based, electronic, images or disc. Legal advice on this agreement should be sought in any case of doubt. It should be applied while following established and agreed processes within the signatory organisations.
- ii. By signing up to this agreement, signatories are committed to a positive approach to information sharing, and agree to meet the outlined commitments and processes.
- iii. It is the responsibility of each signatory to ensure that:
 - Information shared is in accordance with the law
 - Appropriate staff training and awareness sessions are provided in relation to this agreement, and that their organisation abides by the Golden Rules for information sharing (see **Appendix A**)
 - Information is shared responsibly and in accordance with professional and ethical standards
 - Any restrictions on the sharing of the information contained in the disclosure, in addition to those contained within this agreement, should be clearly noted. Information exchanges and refusals are recorded in such a way as to provide an auditable record.
 - Each partner must appoint a Single Point of Contact (SPoC). The sharing of information must only take place where it is proportionate, necessary and legally justified.
 - Requests and replies may be communicated via e-mail should the recipient subscribe to an encrypted email server (pnn, gsi, cjsm, nhs.net and gcsx).
 - This agreement does not give agencies an automatic right to receive or provide information. It is a process for information sharing in cases in where it is suitable to do so.
 - The Police may request a copy of the partner's information security policy (where it exists) when sensitive personal data is to be shared.
 - This agreement may be published on the Hampshire Constabulary external websites for the purposes of openness regarding information sharing within the Police.

4.2 HOW / WHAT INFORMATION WILL BE SHARED

- i. The Police will share :
 - Record Management System (RMS) data
 - Intelligence – the National Probation Service/Police may share MAPPA minutes – risk management plans
 - Hampshire Liaison & Diversion Scheme (HDLS) information (from Custody report to RMS related)
 - Police National Computer data
 - Police National Database data.
- ii. This will be shared during the initial multi-agency meeting which will be held within 5 working days of agreement by the Superintendent. There may be prior information sharing depending on risk.

iii. The listed signatories will share:

- Mental Health reports/intervention
- Medical information
- Housing records and reports
- Information regarding drug and alcohol use
- Victim Support Services information
- Child/Adult Services reports
- Any other information which is necessary and proportionate in order to formulate a risk management plan and protect the public from harm.

4.3 CONSTRAINTS ON THE USE OF INFORMATION

- i. Any data will only be used for the specific purpose for which it is shared, and recipients will not release information to any third party without obtaining the express written authority of the disclosing partner, including requests from the public, disclosure within judicial proceedings and safeguarding forums.
- ii. All information that is disclosed under this agreement remains the property of the original data owner.
- iii. Information will not be shared where disclosure would prejudice ongoing criminal proceedings unless there is an overriding safety requirement to do so.
- iv. This Agreement does not constitute an overarching permission for the broad, comprehensive or unchallenged sharing of Personal Data. It provides a framework for the sharing of Information which aligns with the objectives set out below.

4.4 RESTRICTIONS ON INFORMATION SUPPLIED

- i. Personal data will only be used for the specific purpose for which it was obtained.
- ii. The recipient of the information is required to store records securely utilising current processes and should retain only as long as necessary. They should be securely destroyed one month after all services in relation to an individual have ended. Files containing information from partner sources will be reviewed and deleted in line with Force policy.

4.5 REVIEW OF THE INFORMATION SHARING AGREEMENT

- i. This ISA will be reviewed, as a minimum, six months after its implementation and every two years thereafter. The ISA should always be reviewed if listed signatory organisations change. Any changes will be signed and verified by the Joint Information Management Unit.

5. BREACHES

- i. Any breaches of security, confidentiality or other violations of shared data must be reported to the owning agency as soon as possible and in any case within 24 hours.
- ii. Any breach of information by a signatory partner is their responsibility. Each agency is accountable for any misuse of information supplied and the consequences of such misuse. Any disclosure of information by an employee made in bad faith, or for motives of personal gain, will be the subject of an internal inquiry and be treated as a serious matter.
- iii. The parties shall provide reasonable assistance as is necessary to each other to facilitate the handling of any data security breach. In the event of a dispute or claim brought by a data subject or the Data Protection Authority concerning the processing of Shared Personal Data against either or both parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

6. SIGNATURES

- i. All agencies that are part of the information sharing process will be, upon signing this agreement, bound to comply with its terms.
- ii. Breaches of this agreement will lead to a review and possible termination of this agreement (including the destruction of all previously shared information).
- iii. The Police Information Management and Information Security Teams will be granted reasonable access to undertake an audit to ensure compliance with this agreement. The signatory can exercise its right under this agreement to audit compliance in relation to its own information shared with the Police.
- iv. Any signatory to this agreement may withdraw on giving written notice to the other Signatories. The withdrawing signatory will be bound to comply with those relevant terms of this agreement, which remain effective following withdrawal.
- v. Where the Chief Executive or Director leaves the organisation, it is not a requirement to re-sign the ISA. If a signatory changes, contact details of the new SPoC must be circulated in writing to all parties.

APPENDIX A: GOLDEN RULES FOR INFORMATION SHARING

- Confirm the identity of the person you are sharing with
- Obtain consent to share if safe, appropriate and feasible to do so
- Confirm the reason the information is required
- Be fully satisfied that it is necessary to share
- Check with a manager/specialist or seek legal advice if you are unsure
- Do not share more information than is necessary
- Inform the recipient if any of the information is potentially inaccurate or unreliable
- Ensure that the information is shared safely and securely
- Be clear with the recipient how the information will be used
- Record what information is shared, when, with whom, and why; and if you decide not share record your reason.