

INFORMATION SHARING AGREEMENT



INFORMATION SHARING AGREEMENT (ISA)

BETWEEN

Hampshire Constabulary

AND

Domestic Abuse Prevention Partnership (DAPP) and Integrated Domestic Abuse Service for Hampshire (IDASH) Partners (Named Agencies in Section One)

Version 4.3

Date Agreement comes into force:	19/03/2019
---	------------

1. INTRODUCTION 2

2. PURPOSE 2

3. STATUTORY POWERS TO PROCESS PERSONAL DATA 3

4. PROCESS 5

4.1 THE AGREEMENT 6

4.2 HOW / WHAT INFORMATION WILL BE SHARED 7

4.3 CONSTRAINTS ON THE USE OF INFORMATION 7

4.4 RESTRICTIONS ON INFORMATION SUPPLIED 8

4.5 REVIEW OF THE INFORMATION SHARING AGREEMENT 8

5. BREACHES 8

6. SIGNATURES 9

APPENDIX A: GOLDEN RULES FOR INFORMATION SHARING 10

1. INTRODUCTION

- i. The Police are committed to tackling Crime and Disorder and safeguarding citizens across Hampshire and work, on a regular basis, with Domestic Abuse Prevention Partnership (DAPP) partners in order to make Hampshire Constabulary safer and provide a framework for action.
- ii. This Agreement concerns itself with arrangements surrounding the management of cases referred to the DAPP for the flagging of priority perpetrator management by the relevant agencies.
- iii. The Hampshire DAPP was developed following the commissioning of domestic abuse services for perpetrators by Hampshire County Council, Southampton City Council and the Office of the Police and Crime Commissioner for Hampshire and the Isle of Wight.
- iv. The signatories to this agreement will represent the following agencies/bodies:
 - The Hampton Trust
 - Baseline Consultancy
 - Aurora New Dawn
 - Hampshire County Council
 - Southampton City Council
 - Yellow Door (Southampton Services)
 - Sub-contractors to Yellow Door Services
 - YOU Trust
 - Stop Domestic Abuse.
- v. This agreement should also be used to further clarify any current arrangements.
- vi. 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 a full assessment of risks and appropriate provision of management in cases involving individuals who have been engaging in priority perpetrator behaviour. With access to the data shared under this agreement a more complete assessment can be conducted. The agencies involved with managing the risk can then seek to prevent reoffending or direct the appropriate level of support and care to victims. Through this agreement, the DAPP Partnership will:
- Assist with the collection, referral, exchange and gathering of relevant information during meetings
 - Facilitate consultation between agencies during the referral and suitability decision making process, particularly in reference to priority perpetrators
 - Facilitate intervention by the relevant agencies as early as possible
 - Facilitate a coordinated approach that targets crime and anti-social behaviour
 - Contribute to ongoing effective risk management
 - Uphold compliance with statutory requirements
 - Improve the overall liaison between agencies
 - Monitor information sharing processes and their effectiveness.
- iv. It should be noted that the principles on which the DAPP priority perpetrator management will be run are directly analogous to those governing Multi Agency Risk Assessment Conference (MARAC) meetings. This Information Sharing Agreement will discuss how information will be deemed proportional and necessary to be shared at these meetings.
- 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

The principle legislative instruments that provide powers to lawfully share information under this agreement are:

- i. **The General Data Protection Regulations 2018:** Hampshire Constabulary processes personal information in accordance with this legislation, which exists to ensure the fair and lawful use of personal data and to protect the rights of the data subject. The Regulations provide exemptions to some of its provisions if complying with them will prejudice the protection/detection of crime and the apprehension and prosecution of offenders. This legislation also requires Hampshire Constabulary to comply with the following principles when processing personal data:
- Fairly and lawfully processed;
 - Being processed for specified and lawful purposes and not in any manner incompatible with those purposes;
 - Adequate, relevant and not excessive;
 - Accurate and where necessary, up to date;
 - Not kept for longer than is necessary;

- Being processed in accordance with individuals rights;
 - Secure;
 - Not to be transferred to countries outside the EU.
- ii. **The Human Rights Act 1998:** Hampshire Constabulary 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 or her private and family life, home and correspondence by a public authority. Interference of this right by Hampshire Constabulary 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. **Rehabilitation of Offenders Act 1974:** Sharing of personal data relating to criminal record data must comply with this act which places prohibitions on the use of criminal record data.
- iv. **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.”*
- 2.2.2. 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.
- v. **Sharing personal data for 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.
- vi. 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.

- vii. Each party shall ensure that it processes the Shared Personal Data fairly and lawfully and ensure that it processes the Shared Personal Data on a lawful basis.
- viii. This agreement coincides with the Police and Crime Commissioner's Plan of aiming to bring together those organisations who share the common goal of reducing crime and preventing reoffending. This is evident within the Police and Crime Plan 2017 – 2021¹:
 - Pillar One: Championing Community Needs: To ensure that appropriate services are in place to protect and support victims and those affected by crime through the provision of specialist support for victims of domestic and sexual abuse.
 - Pillar Four: Reduce Re-offending: Priority perpetrators will not necessarily be flagged within the Integrated Offender Management model, as they are not responsible for 'volume crime' or not necessarily known to Criminal Justice Service agencies. However the victim/s is subject to a series of incidents, but the crime recording system will record it as one incident when reported. Likewise they may not be within the Multi Agency Public Protection Arrangements (MAPPA) system. Triggers for priority perpetrators can include alcohol and drugs, and therefore signposting to rehabilitation services may also be relevant.

4. PROCESS

- i. 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.
- ii. **Referral Stage and Identification of Cases**

Referrals will be received from DAPP partners, Hampshire Constabulary (specifically Multi Agency Risk Assessment Conference, High Risk Domestic Abuse, Multi Agency Tasking and Co-ordination, Neighbourhood Policing Teams and Intelligence Tasking and Development), Integrated Domestic Abuse Service for Hampshire (IDASH) providers, Youth Offending Service, Community Rehabilitation Companies, National Probation Service, Children's Services and sexual violence services. Other agencies will be responsible for determining which perpetrators constitute a risk and require assessment for tracking. Any Criminal Justice Service (CJS) agency may also refer cases via contact with offenders and victims in the course of their work.

A designated Coordinator from Aurora New Dawn will have access to the Police Record Management System (RMS) in order to research priority perpetrators which have been referred by multi-agency partners. In the event of a category three Multi Agency Public Protection (MAPPA) referral, the Aurora New Dawn Coordinator may request for a Hampshire Constabulary employee to undertake a Police National Computer (PNC) check. The highest risk cases will be tracked for a three month period and relevant information will be collated from police systems in order to assess and/or reduce risk and manage each case appropriately. The referral data and information from RMS will be kept within SafetyNet and recorded on a secure spreadsheet summarising the referring agency, date of referral, Safetynet case number, Priority Perpetrator Identification Tool (PPIT) information and which DAPP agency is the lead for managing the perpetrator. RMS information may include names, dates of birth, ethnicity, number of victims for a given perpetrator and occurrence numbers.

¹ <https://www.hampshire-pcc.gov.uk/plan> (Page 11-12)

The Aurora New Dawn Coordinator will set up “Notify If” markers on RMS within perpetrator records. This will ensure a notification is sent to the Coordinator if a perpetrator is linked to a new occurrence.

iii. **Consultation**

Case consultation will be provided by the Aurora New Dawn priority perpetrator co-ordinator and will consist of a review of tracked cases and provision of advice in relation to the information given. At all times case responsibility lies with Aurora New Dawn, Police and/or Probation.

iv. **Case Formulation**

These will be completed in the most complex cases where the objective is to provide an explanation of the person’s problem behaviour which will aid sentencing, treatment and management plans. This will include a hypotheses about the onset, motivation and maintenance factors about the person’s behaviour and functioning. These will be provided in the form of a written formulation. This is likely to be a paper based exercise, although in certain cases an interview approach may be possible.

v. **Risk Assessment**

Formal risk assessments will be carried out using PPIT (Priority Perpetrator Identification Tool). These will be arranged between the DAPP partners and Offender Management Hub depending on priority.

vi. **Disclosure to Victim**

It is recognised that there will be occasions whereby it will be in the best interests of potential victims to be informed of behaviour they are unaware of. The amount of disclosure in such cases will be assessed and dealt with on a case by case basis and managed by the DAPP and Police service, by and/or in close liaison with the relevant case officer.

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, cjsm and nhs.net).
- 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.
- Hampshire Constabulary 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 Constabulary.

4.2 HOW / WHAT INFORMATION WILL BE SHARED

- i. To prevent irrelevant or excessive information being disclosed, the data which may be shared under the terms of this agreement as part of the initial referral can consist of:
 - Name, date of birth and address of perpetrator/victim
 - Details of priority perpetrator behaviour/relevant offending behaviour relating specifically to Domestic Violence and/or MAPPA offences
 - Any other relevant or antecedent material necessary for undertaking a full and informed assessment, including any historical mental health issues or weapon warning markers.
- ii. This data will only be shared securely through CJSJ email.
- iii. A designated Coordinator for Aurora New Dawn will have access to the Police Record Management System (RMS) in order to research priority perpetrators which have been referred by information sharing partners. This access will be sponsored by a senior officer or member of staff within Hampshire Constabulary.
- iv. The designated Coordinator from Aurora New Dawn will share only the summary of MARAC meeting minutes with The Hampton Trust. Any further information must be requested through a DP5 form to Hampshire Constabulary.

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 retained for five years from the date of the most recent referral and securely destroyed thereafter. Files containing information from partner sources will be reviewed and deleted in line with Force policy.
- iii. Data will be reviewed manually for deletion by the Aurora New Dawn co-ordinator.

4.5 REVIEW OF THE INFORMATION SHARING AGREEMENT

- i. This ISA will be reviewed, as a minimum, 6 months after its implementation and every year 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. Hampshire Constabulary 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 Constabulary.
- 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.