

INFORMATION SHARING AGREEMENT



HM Prison &
Probation Service



Southern Health
NHS Foundation Trust

Hampshire
& Isle of Wight
Community Rehabilitation Company



An Interserve-led company

Hampshire Stalking Clinic Multi-Agency Stalking Intervention (ISA)

BETWEEN

Hampshire Constabulary

AND

**Aurora New Dawn
National Probation Service (NPS)
Southern Health NHS Foundation Trust
Hampshire & Isle of Wight Community Rehabilitation Company(CRC)
Version 1.3**

Date Agreement comes into force:

1st September 2018

1.	INTRODUCTION	3
2.	PURPOSE	3
3.	STATUTORY POWERS TO PROCESS PERSONAL DATA	4
4.	PROCESS	6
4.1	<i>THE AGREEMENT</i>	<i>6</i>
4.2	<i>HOW / WHAT INFORMATION WILL BE SHARED</i>	<i>7</i>
4.3	<i>CONSTRAINTS ON THE USE OF INFORMATION</i>	<i>8</i>
4.4	<i>RESTRICTIONS ON INFORMATION SUPPLIED</i>	<i>8</i>
4.5	<i>REVIEW OF THE INFORMATION SHARING AGREEMENT</i>	<i>8</i>
5.	BREACHES	8
6.	SIGNATURES	9
	<i>APPENDIX A: GOLDEN RULES FOR INFORMATION SHARING</i>	<i>10</i>

1. INTRODUCTION

- i. The Police are committed to tackling Crime and Disorder and safeguarding citizens across Hampshire and work, on a regular basis, with members of Aurora New Dawn, Suzy Lamplugh Trust, National Probation Service and Southern Health in order to make Hampshire and the Isle of Wight safer and to provide a framework for action.
- ii. The purpose of this agreement is for the Multi-Agency Stalking Intervention Project (MASIP) to select individuals for an intervention programme which aims at dealing with stalking behaviours and the likelihood of recidivism. The MASIP will incorporate measures aimed at:
 - Facilitating a coordinated approach that targets stalking specific behaviours, identifies intervention opportunities, and supports victims of stalking.
 - Facilitating the collection and exchange of relevant information
- iii. The MASIP is funded by a grant from the Home Office under the terms of a Grant Agreement Ref. PR091-2017 (the **Grant Agreement**). The Mayor's Office of Policing and Crime (**MOPAC**) is the governance partner for the MASIP and the programme manager for the MASIP is The Suzy Lamplugh Trust (the **Trust**).
- iv. The Police and Crime Commissioner for Hampshire (**HPCC**) has entered into a collaborative agreement with MOPAC and the Trust (the **Collaborative Agreement**), which sets out the terms and conditions on which MASIP grant funding shall be made available to the HPCC for the purposes of carrying out the MASIP in Hampshire and the Isle of Wight.
- v. This agreement sets out the framework for sharing personal data between the parties for the purposes of identifying individuals who may require mental health assessment, diversion and treatment. This agreement should also be used to further clarify any current arrangements between the parties.
- vi. 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 as data controllers. 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. Individuals will be referred into the Recolo Project which is being run by Southern Health. Police will identify individuals and will make a referral into the MASIP Referral Meeting via the Police led stalking triage process. The purpose of the programme is to offer different levels of intervention such as psychiatric, psychological and occupational therapy for individuals who have displayed problematic fixated and obsessive stalking behaviours and who meet the criteria for intervention.

- iv. Each data subject will be carefully considered in the context of the referral criteria prior to any transfer of the information from Hampshire Constabulary in order to ensure that the information remains proportionate and necessary for the purpose at all times. Referrals will include those cases which have resulted in no further action being taken following a Police investigation, where the criminal justice process has concluded, and where the subject is currently on an order with National Probation Service. In conjunction, all data held by partner agencies will be carefully reviewed to ascertain whether it can in turn be shared with Hampshire Multi-Agency Stalking Consultancy Clinic on the basis of proportionality and necessity.
- v. Data can only be used for the purpose stated and cannot be shared with third parties without written permission. Information that may prejudice an ongoing investigation will not be shared unless there is an overriding safety requirement.
- vi. This document sets out the way in which this data transfer shall be affected and the factors that shall be considered in doing so.
- vii. The aim of the partnership is to identify individuals who may require mental health assessment, diversion and treatment and who display concerning fixated behaviours. Once identified and reviewed the aim is to address concerns raised by referrals. If deemed appropriate, Southern Health will be supplied with proportionate and relevant information to enable Southern Health intervention, where required, thus addressing policing concerns. The information provided will enable the Southern Health to have a more informed opinion about the mental health of the data subject and to be able to offer appropriate intervention.

3. STATUTORY POWERS TO PROCESS PERSONAL DATA

- i. There is no specific relevant statutory power for the purposes of this agreement.
- ii. 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.
 - Protection of Freedoms Act 2012 Part 11 of Schedule 9
 - Protection from Harassment Act 1997 Section 2A and 4A (PHA 1997)
 - Crime and Disorder Act 1998 Section 32
 - Crime and Victims Act 2004 Section 12
- iii. 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.
- iv. **The General Data Protection Regulation 2018** - The EU has introduced The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) to replace Data Protection Act 1998 effective from 25 May 2018. Hampshire Constabulary (HC) processes personal information in accordance with the Act, which exists to ensure the fair and lawful use of personal data and to protect the rights of the data subject. The Act provides exemptions to some of its provisions if complying with them will prejudice the prevention / detection of crime and the apprehension and prosecution of offenders. The Act requires HC 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

v. **The Human Rights Act 1998:** 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.

vi. **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.

vii. **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 police 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: Article 6(1)(e) 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 controller.

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

This agreement will involve the disclosure of special categories, sensitive personal information. This will include the following categories of information: police information relating to the commission/alleged commission of offences; proceedings relating to offences/alleged offences; physical/mental health.

Condition 9(2)(g) Substantial public interest – 10 prevention/detection unlawful acts

a) Processing is necessary for the purposes of the prevention or detection of an unlawful act.

b) must be carried out without the consent of the data subject so as not to prejudice those purpose, and

c) is necessary for the reasons of substantial public interest

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. Police referrals will be initiated for an internal Police review through the submission of an AD344A Stalking Referral document. This is completed by Police sources. This is reviewed internally by the Offender Management Hub. If a case is identified as requiring further joint agency discussion then it will be taken forward to the stalking meeting. This process is attended by Police, Aurora New Dawn, NPS and Southern Health. Other agencies can also refer cases into the triage process for discussion. The triage will decide if the case will be heard at the stalking clinic, or whether it is suitable for the intervention referral meeting, multi-agency tactical advice, or victim referral.
- iii. Where it is agreed that the matter should be forwarded for the Recolo Project Referral meeting, details will be sent to Southern Health and retained. *Referrals will be discussed at an inter-agency meeting attended by Police, Aurora New Dawn, NPS and Health. The meeting will review referrals to The Recolo Project, agree the data subject for assessment, review assessment/formulation outcomes and discuss next steps for the data subject who have been assessed. Consent will be requested prior to assessment taking place and the type of information that will be shared between agencies at the referral meeting will be explained. It is acknowledged that there may be circumstances where Southern Health will have to share information pertaining to public protection and risk management. In these circumstances decisions will be taken and recorded appropriately. If a decision to share information without consent is made, the person will be informed when it is reasonably practicable to do so.*
- iv. At every stage throughout the process efforts will be made to identify victims of stalking and to offer support via the victim advocacy referral process.

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 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 :

- Names, addresses and contact details of the data subject (in order to establish the identity of the data subject for further investigation where necessary)
- Other relevant demographic information
- photograph of the data subject
- relevant criminal justice history
- Victim contact information
- Information held on police systems that may be relevant in order to provide sufficient background information and form a basis for further investigation and assessment of any concern or threat by the partner agencies. This may include
 - i. Warning markers
 - ii. Intelligence
 - iii. Prior Orders (criminal or civil)

ii. The listed signatories will share:

Mental Health

- Relevant mental health information held on RIO system
- Names and addresses of the data subject (in order to establish the identity of the data subject for further investigation where necessary)
- Relevant information from assessments to allow for multi-agency assessment of risk & plan the most appropriate intervention
- Any developing concerns in relation to behaviour

NPS

- Names and addresses of the data subject (in order to establish the identity of the data subject for further investigation where necessary)
- Relevant information from Offender Assessment (OaSys) Risk Assessments
- Current Orders and requirements (including any licence conditions)
- Any current concerns in relation to behaviour
- Victim information for support from Advocacy service

- Details of Victim Liaison Officer (if applicable)

Aurora New Dawn

- Victim detail
- Background information in relation to offending
- Victim impact
- Current risk concerns

4.3 CONSTRAINTS ON THE USE OF INFORMATION

- 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.
- All information that is disclosed under this agreement remains the property of the original data owner.
- Information will not be shared where disclosure would prejudice ongoing criminal proceedings unless there is an overriding safety requirement to do so.
- 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

- Personal data will only be used for the specific purpose for which it was obtained.
- The recipient of the information is required to store records securely utilising current processes and should retain only as long as necessary. In March 2020, the data will be reviewed and a decision will be made on how long the information will be retained for. Files containing information from partner sources will be reviewed and deleted in line with Force policy.

4.5 REVIEW OF THE INFORMATION SHARING AGREEMENT

- 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

- 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.
- 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.