

INFORMATION SHARING AGREEMENT



INFORMATION SHARING AGREEMENT (ISA)

BETWEEN

Hampshire Constabulary

AND

Portsmouth Business Crime Reduction Partnership (PBCRP)

Version 1.0

Date Agreement comes into force:	18/07/2018
---	------------

CONTENTS

1. INTRODUCTION 2

2. PURPOSE 2

3. STATUTORY POWERS TO PROCESS PERSONAL DATA 2

4 PROCESS 4

4.1 THE AGREEMENT 4

4.2 HOW / WHAT INFORMATION WILL BE SHARED 4

4.3 CONSTRAINTS ON THE USE OF INFORMATION 6

4.4 RESTRICTIONS ON INFORMATION SUPPLIED 6

4.5 OTHER OBLIGATIONS OF THE PBCRP AND ITS MEMBERS 7

4.6 REVIEW OF THE INFORMATION SHARING AGREEMENT 7

5 BREACHES 7

6 SIGNATURES 8

APPENDIX A: GOLDEN RULES FOR INFORMATION SHARING 9

1. INTRODUCTION

- i. The Police are committed to tackling Crime and Disorder across Hampshire and work, on a regular basis, with members of the Portsmouth Business Crime Reduction Partnership (PBCRP) in order to make Hampshire safer and to provide a framework for action.
- ii. The purpose of this agreement is to enable police and the members of the PBCRP to work together to tackle crime and to enable action to be taken against crime and anti-social behaviour within the local authority area. This will assist with the issuing of banning orders by PBCRP. 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
- iii. This agreement should also be used to further clarify any current arrangements.
- iv. 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 (ICO). 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. 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.
- iv. The primary purpose of this agreement is for the Hampshire Constabulary (HC) to assist the PBCRP and associated licensed premises by sharing Police photographs and information, when appropriate to do so. The information provided will be for the purpose of protecting the public and reducing crime and disorder by identifying individuals who commit offences and disorder at, or linked to licensed premises, or those whose actions could be considered unsuitable to visit licensed premises, or those whose actions could be considered unsuitable to visit licensed premises in the future.

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:** 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 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.

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.

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.
 - 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. The Police will appoint two disclosure officers to be the Single Points of Contact (SPOC) for the PBCRP in order to manage both Day Time Economy (DTE) Incidents and Night Time Economy (NTE) Incidents. For DTE incidents an officer from the local NPT will be the SPOC for NTE

incidents an officer from the local Police Licensing Team shall be the SPOC. For the police to disclose any of the above information to the PBCRP, the following criteria will need to be fulfilled:

- ii. If the incident linked to a ban was reported to the Police then it must be recorded on a Police recognised computer system or as an incident on the PBCRP members-only database.
- iii. The release of a Police photo, name, age and address MUST be in the interests of public safety, to preserve order or to prevent crime and disorder. There should be sufficient grounds to suspect the person's involvement in the act for which they have been banned.
- iv. The type of incident MUST justify disclosure. For example, violence, theft, drugs, sexual offences, theft and public order offences; linked to alcohol or licensed premises or linked to crime and disorder within DTE non licensed premises.
- v. The release of Police data shall NOT be limited to persons who have been charged, cautioned or positively disposed of in any other way. The decision to disclose shall be based on all relevant factors in the Police material relating to the incident and to be in the interests of public safety and preventing crime and disorder.
- vi. The person put forward for a PBCRP ban MUST be aged 18 years or over for a photo to be released by the Police. The publication of photographs of those under this age is prohibited by the Children and Young Person's Act 1933.
- vii. The material provided by Hampshire Constabulary MUST be sent to the PBCRP either by hand or directly onto the secure PBCRP online website. E-mail shall not be used unless there is a secure e-mail link in existence between the parties involved. Where physical documents are shared all parties must ensure that these are kept securely and disposed of in the correct manner.
- viii. In order to comply with the fairness and transparent principle under Article 5(1)(a) of the GDPR 2018, the subject must be informed of the disclosure of their details to the PBCRP. Therefore the PBCRP will give written notice of this to the subject.
- ix. If after a person is banned and material has been released by Police, evidence comes to light that the person was not involved or their involvement was acceptable, the disclosure officer should seek to retrieve the disclosed information or ensure that the photo is deleted from the PBCRP website and no longer available for use (this will not prevent the person remaining 'banned' as this will be a decision for PBCRP). Similarly, any other error identified with the accuracy of a disclosure should be notified to PBCRP at the earliest opportunity.
- x. If during the term of the PBCRP ban the subject's appearance changes significantly, it is acceptable for the Police to provide the PBCRP with an updated photo, if the Police possess one.
- xi. It is the responsibility of the PBCRP to ensure that its current members are aware of the terms and requirements of this information sharing agreement. As such a mechanism should be in place to ensure that new licensed premises managers (designated premises supervisors) of member premises become aware of the requirements rather than relying on cascade information from previous managers.
- xii. The Police will share:
 - A Police custody photograph (If available)
 - The subject's name

- The subject's age
- Home address – (if available for the issuing of banning letters)

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. The material provided by Hampshire Constabulary will only be used for the specific purpose of providing information to staff at DTE and NTE premises that are member of the PBCRP in order to uphold a ban.
- Banned persons are advised at the expiry of their ban, via a letter, of it being lifted and the PBCRP reserve the right, upon any further occurrences or incidents to re-instate the subject immediately back onto the banned list for the stipulated period. Once a ban has been lifted the photo and other material provided by Hampshire Police shall be removed from the PBCRP website.
- If a ban period is extended for the sole reason of having breached or attempted to breach the ban by entering a member licensed or retail premises, the retention of the data provided by the Police is authorised.
- At the conclusion of the ban, or any extension as described above, the individual must be removed entirely from the PBCRP system. Files containing information from partner sources will be reviewed and deleted in line with Force policy.
- The recipient will not release the information to any third party.

4.5 OTHER OBLIGATIONS OF THE PBCRP AND ITS MEMBERS

- i. All decisions to ban persons will be made by the PBCRP in line with their internal banning processes. Any information provided by the Police shall be limited to PBCRP members.
- ii. The PBCRP is the Data Controller for the purposes of processing personal data for the Pubwatch scheme. The scheme will therefore ensure that the appropriate registration is made to the Officer of the Information Commissioner for this processing to be undertaken fairly and lawfully.
- iii. Members of the PBCRP will be restricted to DTE and NTE premises who have joined the scheme and have been made aware of this information sharing agreement and are able to comply with its terms and conditions.
- iv. The PBCRP shall ensure that a responsible person from each member premises has a secure username and password to access the section of PBCRP online site. A system shall be in place whereby each responsible person is aware of their responsibility to keep their username and password, photographic images and other material safe, out of sight from the public and only for the use of staff that are on duty.
- v. The PBCRP shall take all reasonable steps to ensure that members abide by the rules of the PBCRP scheme and the protocol relating to the disclosure of material provided by Hampshire Constabulary.
- vi. The PBCRP and its members shall keep all the material provided by Hampshire Constabulary in a private and secure location, or on the members section of the secure PBCRP online website. The photos and information provided by the police shall only be for staff at member premises to view for work purposes. The photos and information shall not be made available for the general public to view in any circumstances.
- vii. The PBCRP shall take steps to ensure that members are aware of the contents of this 'information sharing agreement' so that they are fully aware of the limitations of Police material and expectations of scheme members.

4.6 REVIEW OF THE INFORMATION SHARING AGREEMENT

- i. This ISA will be reviewed, as a minimum, six 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. 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.