

INFORMATION SHARING AGREEMENT



INFORMATION SHARING AGREEMENT (ISA)

BETWEEN

HAMPSHIRE CONSTABULARY

AND

BASINGSTOKE PUBWATCH

Version 1.0

Date Agreement comes into force:

26/09/2018

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 5

4.3 CONSTRAINTS ON THE USE OF INFORMATION 6

4.4 RESTRICTIONS ON INFORMATION SUPPLIED 6

4.5 OTHER OBLIGATIONS OF BASINGSTOKE PUBWATCH 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. Hampshire Constabulary are committed to tackling Crime and Disorder and safeguarding citizens across Basingstoke and work, on a regular basis, with members of Basingstoke Pubwatch in order to make Hampshire safer.
- 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.
 - A Police custody photograph (if available)
 - The subject's name
 - The subject's date of birth
 - Home address (if available for the issuing of banning letters)
- 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 purpose of this agreement is for Hampshire Constabulary (HC) to assist Basingstoke Pubwatch scheme and associated licensed premises by sharing Police photos 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 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. **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.

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. 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

- iii. 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.

The Human Rights Act 1998 - Under Article 8 everyone has the right to respect for their private and family life, home and correspondence and there shall be no interference by a public authority with this right except as in accordance with the law, necessary for public safety, the prevention of crime or disorder, the protection of health or morals or for the protection of the rights and freedoms of others.

The principle of “proportionality” is a common theme that runs through both the European Convention on Human Rights and judgements of the European Court of Human Rights (ECHR). It is explicitly expressed in the limitations contained in Articles 8-11 where it is stated that any interference or restriction of those rights must be lawful and “necessary in a democratic society”.

- iv. 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.
- v. **Sharing personal 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.
 - 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 appoint a disclosure officer to be the Single Point of Contact (SPOC) for the Basingstoke Pubwatch scheme. This would ordinarily be the local Police Licensing Officer responsible for the area.
For the Police to disclose any of the above information to Basingstoke Pubwatch, the following criteria will need to be fulfilled:
- ii. The incident linked to the ban request MUST be recorded on a Police recognised computer system.
- iii. The release of a Police photo, name, date of birth 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 of the material. For example violence, drugs, sexual offences, theft and public order offences, linked to alcohol or 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 Basingstoke Pubwatch 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 Basingstoke Pubwatch chairman utilizing the initial request of information form to ensure continuity, via the identified secure email address (or by hand). Email shall not be used unless there is a secure email link in existence between the parties involved.
- 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 scheme. Therefore Basingstoke Pubwatch will give written notice of this to the subject (can be included in the formal banning notification).
- 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 Basingstoke Pubwatch website and no longer available for use. This will not prevent the person remaining 'banned' as this will be a decision for Basingstoke Pubwatch. Similarly, any other error identified with the accuracy of a disclosure should be notified to Basingstoke Pubwatch at the earliest opportunity.
- x. If during the term of the ban the subject's appearance changes significantly, it is acceptable for the police to provide Basingstoke Pubwatch with an updated photo, if the police possess one.
- xi. The police SPOC can, if invited, attend Basingstoke Pubwatch meetings to facilitate the process. However police will not contribute to any decisions made when scheme members are considering ban requests.

- xii. It is the responsibility of Basingstoke Pubwatch 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.
- xiii. The Police will share:
 - A Police custody photograph (if available);
 - The subject's name;
 - The subject's date of birth;
 - Home address (if available for the issuing of banning letters).

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 after two years. Files containing information from partner sources will be reviewed and deleted in line with Force policy.
- iii. If a ban period is extended for the sole reason of having breached or attempted to breach the ban by entering a member licensed premises, the retention of the data provided by police is authorised.
- iv. At the conclusion of the ban, or any extension as described above, the subject must be removed entirely from Basingstoke Pubwatch system. All physical material supplied must be returned or destroyed and all electronic data pertaining to that individual, including copies, must be deleted from the Basingstoke Pubwatch system.

4.5 OTHER OBLIGATIONS OF BASINGSTOKE PUBWATCH AND ITS MEMBERS

- i. All decisions to ban persons will be made by Basingstoke Pubwatch members. Any information provided by police shall be limited to Basingstoke Pubwatch members
- ii. Basingstoke Pubwatch is the data controller for the purposes of processing personal data for the scheme. The scheme will therefore ensure that the appropriate registration is made to the Officer of the Information Commission for the processing to be undertaken fairly and lawfully.
- iii. Basingstoke Pubwatch shall ensure that a responsible person from each member premises has a secure username and password to access the section of Basingstoke Pubwatch 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.
- iv. Basingstoke Pubwatch shall take all reasonable steps to ensure that members abide by the rules of the scheme and the protocol relating to the disclosure of material provided by Hampshire Constabulary.
- v. Basingstoke Pubwatch and its members shall keep all material provided by Hampshire Constabulary in a private and secure location, or on the members section of the secure Basingstoke Pubwatch online website. The photos and information provided by the police shall only be for staff at member licensed premises to view for work purposes. The photos and information shall not be made available for the general public to view in any circumstances.
- vi. Basingstoke Pubwatch 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 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. 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.