

INFORMATION SHARING AGREEMENT



INFORMATION SHARING AGREEMENT (ISA)

BETWEEN

Hampshire Constabulary

AND

**Hythe Shopwatch
Version 1.0**

Date Agreement comes into force:	08/01/2019
---	------------

- 1. INTRODUCTION 2**
- 2. PURPOSE 2**
- 3. STATUTORY POWERS TO PROCESS PERSONAL DATA 3**
- 4. BANNING CONDITIONS 4**
- 5. THE AGREEMENT 6**
- 6. HOW / WHAT INFORMATION WILL BE SHARED 7**
- 7. CONSTRAINTS ON THE USE OF INFORMATION 7**
- 8. RESTRICTIONS ON INFORMATION SUPPLIED 8**
- 9. REVIEW OF THE INFORMATION SHARING AGREEMENT 8**
- 10. BREACHES 8**
- 11. SIGNATURES 8**

APPENDIX A: GOLDEN RULES FOR INFORMATION SHARING 10

1. INTRODUCTION

- i. Hampshire Constabulary are committed to tackling Crime and Disorder and safeguarding citizens across Hampshire and work, on a regular basis, with members of Hythe Shopwatch in order to make Hythe safer.
- ii. This agreement is designed to facilitate the transfer of custody images and information relating to known troublemakers to Hythe Shopwatch. This will enable member retail premises to make and enforce private banning decisions where necessary, relevant and desired.
- iii. This arrangement therefore also covers briefing the local retail businesses of nominals known to be proficient at committing retail crime, where there is specific information to suggest the area will be targeted. The sharing of photographs enables retail establishments to protect their property through the monitoring of suspects when on their premises and to report to the police where inappropriate conduct or incidents of theft occur.
- iv. The intention is to protect property and to prevent the commission of a crime; it is not to advise or support any action of private banning by any member businesses, this remains the sole decision of the Shopwatch and its members. The information provided will be for the purposes of protecting the public and reducing crime or disorder.
- 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 (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. The purpose of this agreement is to facilitate the sharing of photographs and information to enable action to be taken against crime and anti-social behaviour within and around retail premises in Hythe. 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
 - Supporting the private banning of individuals to prevent known troublemakers from committing repeated offences
- iv. 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 General Data Protection Regulations 2018:** Hampshire Constabulary (HC) processes personal information in accordance with this 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 protection/detection of crime and the apprehension and prosecution of offenders. This Act also 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. **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.
- 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. 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 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:

The General Data Protection Regulations 2018, Article 6 (1) (e), which states:

“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”

The disclosure of personal information is legally justifiable if it falls within one of the defined categories of public interest:

The Public Interest Criteria include:

1. The administration of justice
2. Maintaining public safety;
3. The apprehension of offenders;
4. The prevention of crime and disorder
5. The detection of crime;
6. The protection of vulnerable members of the community.

When judging the public interest, it is necessary to consider the following:

1. Is the intended disclosure proportionate to the intended aim?
2. What is the vulnerability of those who are at risk?
3. What is the impact of disclosure likely to be on the individual?
4. Is there another equally effective means of achieving the same aim?
5. Is the disclosure necessary to prevent or detect crime and uphold the rights and freedoms of the public?
6. Is it necessary to disclose the information to protect other vulnerable people?

vii. In order to lawfully process **special category data**, including ethnic origin, political or religious beliefs, trade union membership, genetics, biometrics, health, sex life or sexual orientation, and for non-Competent Authorities to process criminal data, it is essential to satisfy an additional lawful basis under Article 9 of the GDPR:

- Preventing/detecting unlawful acts

viii. 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.

4. BANNING CONDITIONS

- 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. This section outlines the conditions and criteria under which Hythe Shopwatch decide to bar individuals from member business premises.

- iii. Where processing is necessary to manage the banning of a data subject from member premises and where information is held by Hythe Shopwatch as a result of disclosure by the police, they will give written notice of the disclosure, along with details of the ban, to the data subject.
- iv. The foundation for each ban will be the submission of an incident report from the business reporting the offence. This will be reviewed by Hampshire Constabulary and the details will be checked for accuracy against the police record of the same event. Thus, bans are reliant upon there being a police record of the event on a recognised computer system.
- v. The release of a Police photo, name, DOB, age or address MUST be in the interests of public safety, to preserve order or to prevent crime and disorder. If there are sufficient grounds to suspect that a data subject will attempt to commit violence, theft and public order offences; linked to or targeted against member premises the release of Police data shall be authorised.
- vi. The type of incident MUST justify disclosure. For example, violence, theft, drugs, sexual offences and public order offences; linked to or targeted against member premises.
- vii. 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.
- viii. The decision making process will be fully documented in each case and will thus ensure that disclosure of information is current, accurate and relevant. Hythe Shopwatch will provide a clear audit trail that supports such disclosure with consideration given to the Human Rights of each individual and an account made of the lawfulness of such action; how it is necessary, justified and proportionate. It will be agreed that the wider interests of public safety and the rights of the society at large will, after due consideration of the circumstances of offence and the resultant conviction, outweigh the rights of the individual.
- ix. The material provided by Hampshire Constabulary MUST be delivered to Hythe Shopwatch by hand. Email shall not be used unless there is a secure email link in existence between the parties involved.
- x. Disclosures will be considered in a case by case basis with each individual store and not circulated widely to others as a result of a ban from one.
- xi. If during the term of the ban, the subject's appearance changes significantly, it is acceptable for the Police to provide Hythe Shopwatch with an updated photo, if the Police possess one.
- xii. 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 Hythe Shopwatch database and no longer available for use (this will not prevent the person remaining 'banned' as this will be a decision for Hythe Shopwatch). Similarly, any other error identified with the accuracy of a disclosure should be notified to Hythe Shopwatch at the earliest opportunity.
- xiii. 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 Shopwatch. Therefore the Shopwatch will give written notice of this to the subject.
- xiv. The police will retrieve such data when no longer relevant for the purposes.

- xv. The Police Single Point of Contact (SPOC) can, if invited, attend committee meetings to facilitate the process however will not contribute to any decisions made when considering ban requests. Any error identified with the accuracy of a disclosure should be notified at the earliest opportunity.

5. 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. Where information or a photo about a person under 18 is being considered the threshold for satisfying the above criteria will be much higher and it is anticipated that sharing will only occur in exceptional circumstances. For example: A prolific offender having a significant negative impact; high likelihood of re-offending; sharing is most likely to prevent re-offending; and the disclosure is in the significant public interest.
- iii. This sharing arrangement shall be restricted to the premises in the Hythe area.
- iv. Hythe Shopwatch 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 Shopwatch 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.
- v. Each store will be Data Controller for the data held by them and liable to ensuring that the processing of personal data is in accordance with the principles of the Data Protection Act. Therefore each retail business will be responsible for ensuring that adequate measures are in place to prevent unauthorised or unlawful disclosure and against accident loss of personal data. The Shopwatch 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.
- vi. It is the responsibility of Hythe Shopwatch and member business to ensure that current members and their employees are aware of the terms and requirements of this information sharing agreement. As such a mechanism should be in place to ensure that new managers or designated premises supervisors of a member premises become aware of the requirements rather than relying on cascade information from previous managers.
- vii. 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.
- viii. 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.
- 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.

6. HOW / WHAT INFORMATION WILL BE SHARED

- Where a policing incident is recorded the following information can be shared:
 - A Police custody photograph (if available)
 - The subject's name
 - The subject's DOB or age
 - Residential address (if available for the issuing of banning letters)
 - A modus operandi (if relevant in targeted briefings)
- Only hard copies of information will be shared via hand to hand transfer. Information will not be shared electronically unless a secure connection exists between the parties.

7. 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.

8. RESTRICTIONS ON INFORMATION SUPPLIED

- i. When no longer relevant, and on request, the photograph and other material provided by Hampshire Police shall be returned. No copies will be retained by Hythe Shopwatch.
- 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 or returned once the banning period for a given individual comes to an end. If a ban period is extended for the sole reason of having breached or attempted to breach the ban by entering a member retail premises, the retention of the data provided by the Police is authorised.
- iii. Files containing information from partner sources will be reviewed and deleted in line with Force policy

9. 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.

10. 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.

11. 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.