

INFORMATION SHARING AGREEMENT



INFORMATION SHARING AGREEMENT (ISA)

BETWEEN

Hampshire Constabulary

AND

Saints Foundation
Version 1.0

Date Agreement comes into force:

16/01/2019

1. INTRODUCTION 2

2. PURPOSE 2

3. STATUTORY POWERS TO PROCESS PERSONAL DATA 3

4. PROCESS 4

4.1 THE AGREEMENT 5

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 REVIEW OF THE INFORMATION SHARING AGREEMENT 6

5. BREACHES 6

6. SIGNATURES 7

APPENDIX A: GOLDEN RULES FOR INFORMATION SHARING 8

1. INTRODUCTION

- i. The Police are committed to tackling Crime and Disorder and safeguarding citizens across Southampton and work, on a regular basis, with members of the Saints Foundation in order to make Hampshire Constabulary safer and to provide a framework for action.
- ii. This agreement will assist in the provision of Early Intervention Programmes for young people who have been identified as at risk of offending.
- iii. This agreement should also be used to further clarify any current arrangements.
- iv. 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 as independent 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. The purpose of this agreement is facilitate the delivery of a high quality, desistance based, Early Intervention Programme which supports excellent outcomes for young people who are identified to be at risk of offending. This will enable action to be taken against crime and anti-social behaviour within the local authority area. It will incorporate measures aimed at:
 - Facilitating a coordinated approach and developing monitoring strategies which targets crime and anti-social behaviour.
 - Facilitating the collection and exchange of relevant information
 - Supporting youth diversion services, namely the Saints Foundation programme.
- iv. The personal data shared as a result of this agreement must not be used for any other reason than the purpose outlined above.
- v. Courses are organised by Saints Foundation every twenty-four weeks for ten youths at a time. Information will be shared at the beginning of the course to assist in the diversion scheme.
- vi. Information will also be shared in instances where a course attendee drops out of the course and is replaced by another, or where additional individuals are referred onto the diversion course.
- vii. Data can only be used for the purpose shared and cannot be shared to third parties (excluding Southampton Youth Offending Service, who the parties agree is an important part of this arrangement and who both parties will communicate with) 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 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) (a), which states:

“The data subject has given consent to the processing of his or her personal data for one or more specific purposes”

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. Article 9 (2) (a) states as follows:

“The data subject has given explicit consent to the processing of those personal data for one or more specific purposes”

The Diversion courses issued by the Saints Foundation may include children under the age of 16, therefore in such instances where consent is obtained, in line with Article 8 (1), consent must be:

“Given or authorised by the holder of parental responsibility over the child”

Alternatively, in instances where an individual is required to attend a program as a result of a youth or court order, personal, sensitive or criminal data may be processed on the basis that there is a legal obligation to do so. As is identified in the Data Protection Act 2018, Schedule 1, Part 3:

“The condition is met if the processing is necessary when a court or tribunal is acting in its judicial capacity”

- vii. 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. 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. Hampshire Constabulary will proactively compile information related to those which have committed, or are on the verge of committing, anti-social behaviour.
- iii. Hampshire Constabulary will, where appropriate, obtain the consent of the parents of young individuals, aged 12-15, and will be informed that, should they consent, their data will be transferred to the Saints Foundation.
- iv. The Saints Foundation will receive the initials of those attending the course by email, which will be stored on a secure cloud based system.
- v. All personal data shared with Saints Foundation will be stored by Saints Foundation in a secure folder for no longer than two years from the date that the data subject leaves or completes the programme.

- vi. Where an individual consents to the sharing of information they will be contacted by the Saints Foundation to undergo a diversion course.
- vii. Where an individual does not complete a course, their name will continue to be held securely for archiving purposes, however, all other personal data will be deleted.

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 information which will be shared under this agreement will include:
 - Name
 - Date of Birth
 - Warning marker/s
 - The reason for referral, including anti-social behaviour or any history of violence
 - Information relating to any out of court disposal issued (where relevant)

- ii. This data will only be shared between parties via encrypted USB or by physical transfer of documents.
- iii. Where information is shared through a hard copy, paper format it should be transferred to a secure computer system and securely disposed of immediately.

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 (other than the Southampton Youth Offending Service) 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.

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 partner agency as soon as possible and in any case within 24 hours of becoming aware that a breach has occurred.
- 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 without undue delay, 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.