

INFORMATION SHARING AGREEMENT



INFORMATION SHARING AGREEMENT (ISA)

BETWEEN

Hampshire Constabulary

AND

University of Portsmouth

Version 4.4

Date Agreement comes into force:	12/11/2018
---	------------

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

APPENDIX A: GOLDEN RULES FOR INFORMATION SHARING 8

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 University of Portsmouth in order to make Hampshire safer.
- ii. This agreement is designed to facilitate the lawful exchange of information in order to support partnership working between Hampshire Constabulary (HC) and the University of Portsmouth (UoP), for the purposes of preventing the commission of offences, bringing offenders to justice and safeguarding students and staff from harm whilst on campus and when resident in University accommodation. It also identifies where other mechanisms exist to facilitate an exchange of information for the same basic aims.
- 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 Regulation (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 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 prevent the commission of offences, bringing offenders to justice, as well as facilitating support for ongoing investigations being carried out by the constabulary. The agreement will also assist in safeguarding students and staff from harm whilst on campus, and when resident in UoP accommodation. Ultimately, this agreement 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 that targets crime and anti-social behaviour.
 - Facilitating the collection and exchange of relevant information.
- 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 Human Rights Act 1998:** Both HC and UoP as public authorities, are duty bound to act in compliance with the Human Rights Act. Article 8 states that everyone has a right to respect for their 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 under the General Data Protection Regulation (Part 2 of the Data Protection Act 2018):**
Where the sharing of personal data is between the Hampshire Constabulary and other Non-Competent Authorities, and /or
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 (Article 6(1)(e) of the GDPR)

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

- Preventing/detecting unlawful acts (DPA 2018 Schedule 1, Part 2 (s)10)

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.

- i. Prior to sharing:
- Assess Risk to students, staff or to the data subject themselves.

- Assess stage of investigation - conviction = high risk / charge = medium risk/ pre-charge = low risk.

A caution or conviction is a clear admission or finding of guilt, while disclosures at the pre charge stage will only generally be made where the risk of harm is commensurately high.

ii. When sharing data:

- Ensure the request for data meets the joint purpose and has come from a legitimate source
- Ensure the partner has enough data to act upon
- Remove excessive data
- Check email chains to ensure excess data is not sent to a recipient in error
- Ensure the accuracy of data
- All requests from the University will outline the purpose/intended aim as well as the information sought, and will be submitted via the official form DP5
- All requests from Hampshire Constabulary will be made in writing on a Declaration Form for Data User (DP2). This will be sent via email. DP2 requests can also be sent via post or delivered in person to University House, Winston Churchill Ave, Portsmouth PO1 2UP.

iii. Keep a record of¹:

- The request for data
- What information has been shared
- Who the information was shared with
- The purpose for sharing
- The rationale for disclosing data, withholding data or declining a request in full.

5. THE AGREEMENT

- 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.
- 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.
- 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

¹ Using the Z Information Sharing (Management Occurrence) on Hampshire Constabulary's RMS or in UoP files

- 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).
- It is understood that this agreement does not give agencies an automatic right to receive or provide information. It is a process for information sharing in cases 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

The Constabulary will share :

- Information regarding crime incidents on University property where the University is the victim of crime; where offending on University property places students or staff at risk of harm; or where serious offending or alleged offending off campus suggests students or staff could be at risk of serious harm.
- Details shared can include personal data and special category data including names, dates of birth and, the nature of offending/alleged offending where relevant
- Special category data such as mental health information and any other information of a medical nature, could also be shared where an individual poses a potential risk to themselves, or to others.
- Information may also be shared in line with a Community Resolution, if notification is agreed by the subject and the victim of crime, and forms part of the Resolution. Community Resolution in this ISA refers to low level application of mediation practices which will be done in line with the Universities code of student behaviour and will engage appropriately vetted staff to facilitate this practice.

The University (UoP) will share:

- Intelligence or information that assists with the investigation of crime occurring on their property
 - Intelligence or information that assists with the investigation of crime involving their students within the local area.
- iii. Information will be shared electronically in cases of operational emergency and with appropriate security safeguards.

7. 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.

8. 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 one (1) year or in line with the applicable retention policies of the parties to this agreement². 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 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.

10. BREACHES

- i. Any breaches of security, confidentiality or other violations of shared data must be reported to the owning party as soon as possible and in any case within 24 hours of the party becoming aware of the breach.
- 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.

² UoP retain the DP2 and any nil response for 1 year, and, 3 years where data has been provided.

- 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 Information Commissioner's Office, 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.