

INFORMATION SHARING AGREEMENT



INFORMATION SHARING AGREEMENT (ISA)

BETWEEN

Hampshire Constabulary

AND

**Victim Support
DriveTech (UK) Limited trading as DriveTech
Version 2.0**

Date Agreement comes into force:	14/09/2018
---	------------

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 REVIEW OF THE INFORMATION SHARING AGREEMENT 6

5. BREACHES 7

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 Hampshire and work, on a regular basis, with members of DriveTech and Victim Support in order to make Hampshire safer and to provide a framework for action.
- 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 is not covered by this agreement.
- iv. The purpose of this agreement is to facilitate a booking process for Victim Awareness Courses (VAC) for data subjects who have explicitly accepted a conditional caution or a community resolution with a condition to attend a course. On booking the course, the details of the data subject are to be passed to Drivetech, who will provide Victim Support with online portal access to assist in the processing of data. DriveTech and Victim Support will then report course attendance back to Hampshire Constabulary (HC). 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 that targets crime and anti-social behaviour.
 - Facilitating the collection and exchange of relevant information.
- 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.

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:** HC processes personal information in accordance with these regulations, which exists to ensure the fair and lawful use of personal data and to protect the rights of the data subject. The legislation 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. These regulations 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. 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 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?

- vi. 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:
 - 2(g) Processing is necessary for reasons of substantial public interest.
- 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. HC will provide the Data Processors with details of offenders who have explicitly accepted a conditional caution or community resolution with a condition to attend a course. This will be sent on a weekly basis.
- iii. The Processors will contact the offender via telephone, letter or email to facilitate the booking of a Victims Awareness Course.
- iv. Payment for the course can be collected from the individual by the Processors making the contact.
- v. Once a course has been completed, the Data Processor will report this to HC through secure email.

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. Only those employees who have been appropriately checked through the completion of Disclosure & Barring Service (DBS) Checks will have access to Police data.
- iv. 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

- The information which will be shared under this agreement will be shared on a weekly basis with DriveTech via Criminal Justice Secure email (CJSM) and will include details relating to offenders who are required to attend a Victim Awareness Course.
- DriveTech will provide Victim Support with access to their portal, through which the data can be viewed and processed.
- Victim Support will report compliance to HC on a weekly basis through CJSM.
- The Data Processors can share relevant information, including names, alternative addresses, telephone numbers or email addresses between themselves to fulfil the purpose of contacting data subjects to complete a Victim Awareness Course.
- The information which will be shared will be as follows:

From HC to the Data Processors:

- Police reference number;
- Title;
- Name;
- Address details;
- Contact details, including telephone number and email address;
- Offence type;
- Offence date;
- Critical date of case;
- Special requirements.

The following information will be sent from the Data Processors to the Data Controller for those who have successfully completed a course:

- Name;
- Police reference number;
- Date course completed.

For those that are not engaging or who have failed to complete a course within their critical date, the Data Processor will share:

- Name;
- Police reference number;
- Details of any attempts to book onto a course.

If on the initial transfer of data to DriveTech information is missing or inaccurate, the Data Controller will send to Victim Support the following information:

- Addresses;
- Phone numbers;
- Email addresses;
- Special requirements.

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.
- v. DriveTech will become the Data Controller of additional data which is provided to them directly by the data subject.

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 three 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 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 all 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.