

INFORMATION SHARING AGREEMENT



INFORMATION SHARING AGREEMENT (ISA)

BETWEEN

Hampshire Constabulary

AND

Boomtown Fair 2019

Version 1.0

Date Agreement comes into force:

1st August 2019

1. INTRODUCTION 2

2. PURPOSE 2

3. STATUTORY POWERS TO PROCESS PERSONAL DATA 3

4. PROCESS 5

4.1 THE AGREEMENT 6

4.2 CONSTRAINTS ON THE USE OF INFORMATION 7

4.3 RESTRICTIONS ON INFORMATION SUPPLIED 7

4.4 REVIEW OF THE INFORMATION SHARING AGREEMENT 7

5. BREACHES 7

6. SIGNATURES 8

APPENDIX A: GOLDEN RULES FOR INFORMATION SHARING 9

1. INTRODUCTION

- i. The Police are committed to tackling Crime and Disorder and safeguarding citizens across Hampshire and work on a regular basis with the organisers of Boomtown Fair in order to make Hampshire safer and provide a framework for action.
- ii. This Information Sharing Agreement has been produced by Hampshire Constabulary to work with the music event organiser to assist the appropriate sharing of information to enable action to be taken against crime and anti-social behaviour within the local authority area. It will incorporate measures aimed at:
 - Increasing the confidence of visitors to the organised event
 - Increasing the confidence of residents living in the immediate area of the organised event
 - Maintaining crowd safety
 - Facilitating a coordinated approach that targets crime and anti-social behaviour.
 - Facilitating the collection and exchange of relevant information
 - Assisting in the pursuit of civil and criminal proceedings
 - Ensuring that the sharing of information meets one of more policing purposes
 - Ensuring that the sharing of information allows both partners to make informed decisions on risks throughout the duration of the festival
- iii. This agreement is mainly concerned with the exchange of personal information. Therefore, where de-personalised information is requested the assumption is that this information will be shared. Wherever possible, information that does not identify individuals should be used and disclosed.
- iv. This agreement will also be used to further clarify any current arrangements. However, it must be recognised that this document cannot provide clear guidance on every type of scenario and should be used only as an overall guide. As each “case” must be treated on its own merit, it may be necessary for organisations to seek specialist advice before requesting or disclosing any personal information.
- v. The disclosures stemming 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 as 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. To prevent irrelevant or excessive information being disclosed, the type of information that may be shared under the terms of this agreement by the event organisers can consist of:
 - names, addresses, images, modus operandi and vehicles used;
 - associated suspects in relation to the commission of crime and disorder including details of persons ejected from the site;

- Details of non-ticket holders trying to gain access to the site to ensure all intelligence is captured.
- Potential and actual fence breaches (depersonalised data)
- Traffic and pedestrian patterns (depersonalised data).

Hampshire Constabulary may share:

- Sanitised details of stop checks to be shared with stakeholders during debrief;
 - Information relating to arrests;
 - Post event intelligence and crime analysis, following thorough sanitisation;
 - Reports of incidents;
 - Information relating to drug use, drug dealing and the effects of drugs discovered off site;
 - Intelligence from the ACPO Music Festival Working Group, Operation Gothic
 - Community information, including the impact on the local community (depersonalised data);
- Information will not be shared where disclosure would prejudice ongoing criminal proceedings unless there is an overriding public safety requirement to do so.
 - Hampshire Constabulary can share where necessary and proportionate to meet the policing purpose
 - With access to the data shared under this arrangement, festival organisers and its security will be able to take appropriate action to manage risks or report relevant concerns to the police in order to safeguard festival goers and local residents.
 - The parameters of the agreement will also allow the two agencies to work in partnership for the benefit of the wider public interest in reducing crime, preventing crime and anti-social behaviour which are encompassed by the Crime and Disorder Partnership.
 - 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.
 - No police tactics will be shared under this agreement

3. STATUTORY POWERS TO PROCESS PERSONAL DATA

- The principle legislative instruments that provide powers to lawfully share information under this agreement are:
- 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. Each party shall ensure that it processes the Shared Personal Data fairly and lawfully and ensure that it processes the Shared Personal Data for the following lawful bases:

v. **Sharing personal data for the Law Enforcement Purpose (under Part 3 of the Data Protection Act 2018):**

Where the sharing of personal data is between the police and other Competent Authorities (as defined by Schedule 7 of the Data Protection Act 2018) for any of the Law Enforcement purposes (prevention, investigation, detection, prosecution of criminal offences, execution of criminal penalties, safeguarding against and preventing threats to public security) the following lawful basis applies for the processing of special categories of personal data:

- A function conferred by enactment or rule of law, necessary in the substantial public interest

vi. **Sharing personal data under the General Data Protection Regulations (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. Article 9 (2) (g) states as follows:

“Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject”

As is described in Schedule 1, Part 2 (10) in the Data Protection Act 2018, the disclosure of special category data is necessary when the condition of preventing of detecting unlawful acts is met:

(1) This condition is met if the processing—

(a) is necessary for the purposes of the prevention or detection of an unlawful act,

(b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and

(c) is necessary for reasons of substantial public interest.

(2) If the processing consists of the disclosure of personal data to a competent authority, or is carried out in preparation for such disclosure, the condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).

(3) In this paragraph—

(i) “act” includes a failure to act;

(ii) “competent authority” has the same meaning as in Part 3 of this Act (see section 30).

- 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. 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. All requests for police data should be made by the event organiser, or persons under their command, for the purposes of this agreement.

- iii. The request for information sharing must contain:
 - The reason for the request
 - The relevance of data sought to the request
 - The data requested
 - Any necessary information which can assist in identifying the data sought.
- iv. The identity of the originator must be recorded against relevant data.
- v. 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
 - Double check all email addresses before sending
- vi. 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.

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).

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

- 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 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.

4.3 RESTRICTIONS ON INFORMATION SUPPLIED

- Personal data will only be used for the specific purpose for which it was obtained.
- 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 once the ISA is no longer in use. Files containing information from partner sources will be reviewed and deleted in line with Force policy.

4.4 REVIEW OF THE INFORMATION SHARING AGREEMENT

- This ISA will be reviewed, as a minimum, 6 months after its implementation and every one 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

- 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.
- 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.
- iv. In the event of loss or error:
 - Establish the facts of the loss or compromise
 - If possible, identify where the data is or who it has gone to
 - Identify the data which has been compromised
 - Inform your Information Security Officer.

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.