



Information Sharing Agreement

**Chief Constable of Thames Valley Police
and the
Police and Crime Commissioner for Thames Valley**

1. Introduction

This information Sharing Agreement ("ISA") has been developed between the Chief Constable of Thames Valley Police ("TVP") and the Police and Crime Commissioner for Thames Valley ("the PCC"¹), hereafter termed "parties" to explain;

- Why the parties have agreed to share information;
- The legal justification behind the sharing;
- Who, on behalf of each party, has managerial oversight and responsibility for the information sharing;
- The principles by which information will be shared and used;
- How miscellaneous matters will be managed.

For the purposes of this ISA the term "sharing" information means providing or disclosing information to the other party by any means.

Information shared under this ISA will comprise of some information that is defined as "personal data" under Part 1, Section 3 of the Data Protection Act 2018 ("DPA") and this ISA helps support both parties' compliance with that Act and with the UK General Data Protection Regulation ("UK GDPR").

2. Why the parties have agreed to share information

The Police Reform and Social Responsibility Act 2011 created the role of PCCs for police force areas in England and Wales and set out the functions that the PCCs must discharge.

In order for the PCC to discharge those functions there is a requirement for information in the possession of TVP to be shared with the PCC. A reciprocal sharing of information from the PCC to TVP may also be required to assist in the discharge of the PCC's or Chief Constable's functions or for policing purposes.

This ISA is not intended to cover a) information sharing between the PCC and the Thames Valley Police and Crime Panel or b) information sharing between the Chief Constable of TVP and the Thames Valley Police and Crime Panel.

3. How the sharing can be legally justified

The legal justification for the sharing of information between TVP and the PCC is derived from the Police Reform and Social Responsibility Act 2011 ("the PRSRA") and the "Policing Protocol" (SI 2011/2744).

According to paragraph 19 of the Policing Protocol:

"In order to enable the PCC to exercise the functions of their office effectively, they will need access to information and officers and staff within their force area. Such access to any

¹ For the purposes of this ISA the term PCC is used to encompass the person elected as the PCC and any staff authorised to work for or on their behalf or under their direction and control (ie. The Office of the Police and Crime Commissioner or "OPCC").

information must not be unreasonably withheld or obstructed by the Chief Constable and/or fetter the Chief Constable's direction and control of the force."

It is accepted and agreed by both parties that it may be necessary to share information in order to enable the PCC and/or the Chief Constable to discharge his/her statutory functions and/or for a policing purpose.

The sharing of personal data is governed by the UK GDPR (in particular Articles 6 and 9), in the case of non-law enforcement processing. Both parties acknowledge and agree that any sharing of personal data must be justified on a case-by-case basis in accordance with those provisions; and in particular that any sensitive processing, or processing of special category data, must be justified by reference to the conditions in Schedule 8 of the DPA, or Article 9 of UK GDPR, as the case may be.

Whilst the lawful basis will be dependent on the purpose for sharing, both parties will mainly be relying on:

- **(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose. (E.g. If an individual contacts the OPCC regarding operational matters and provides consent for us to pass this to TVP).
- **(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations). (E.g. If the OPCC receive a complaint where TVP are the appropriate authority in law, the OPCC have a duty in law to pass this on).
- **(d) Vital interests:** the processing is necessary to protect someone's life. (E.g. If a member of the public threatens to harm themselves, the OPCC would share their personal data with TVP).
- **(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

It is important to note that most of the sharing will be undertaken as relying on (e)Public Task, the other basis' will be used by exception such as in the examples provided above.

In relation to special category data, again, the lawful basis will be dependent on the purpose for sharing, with both parties mainly relying on:

- (a) Explicit consent
- (c) Vital interests
- (f) Legal claims or judicial acts
- (g) Reasons of substantial public interest (with a basis in law)

And also Schedule 1, Part 2(6) of the DPA- Statutory and Government Purposes.

4. Managerial Oversight for the Information Sharing

Managerial Oversight of the information sharing under this ISA will be conducted by the individuals identified in the following paragraphs.

In the case of the Chief Constable of TVP: the Chief Information Officer

In the case of the PCC: the Chief of Staff

However, the departments responsible for the management of this ISA and ensuring compliance with it on behalf of the above are:

In the case of the Chief Constable of TVP: The Joint Information Management Unit.

In the case of the PCC: The Governance Team.

The above departments will be responsible for the periodical revision of the ISA as working practices are developed and refined.

Sharing of information on a day-to-day basis under this ISA will generally be undertaken by the methods described in Section 6.

It is noted by the parties that the PCC retains a residual power to require the provision of certain information pursuant to Section 36 of the PRSRA. This agreement is made without prejudice to the exercise of that power although given the principles agreed herein it is not envisaged that the power will be routinely used.

5. Information that may be shared

Any information within the possession of TVP or the PCC may be considered for sharing with the other party to this ISA, provided that it is lawful; necessary, relevant and not excessive for that purpose. This can include, and is not limited to:

- Operational data,
- Complaint files,
- Statistics,
- HR records,
- ICT records etc.

Information will be shared between TVP and the PCC where all of the following apply:

- The sharing is reasonably required by the OPCC or TVP to assist the PCC or the Chief Constable in exercising his/her statutory functions,
- The sharing would not prejudice ongoing or potential investigations or prosecutions by TVP or other parties,
- The sharing would not contradict any legal obligation upon TVP or the OPCC that prohibits or precludes sharing,
- The data held by both TVP and the OPCC should be held in a way that is electronically compatible with each other, and
- Any information shared must abide by the 7 principles contained within the UK GDPR and the DPA being:-
 - Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject;
 - Sharing of personal data should be for specified and legitimate purposes;
 - The data you share should be adequate, relevant and limited to what is necessary;
 - The data you hold must be accurate and where necessary kept up to date;
 - The date you hold must be kept in a form which permits identification of data subjects for no longer than is necessary;
 - The data you hold must be processed in a manner that ensures appropriate security of the personal data.

- Each party is responsible for complying with the UK GDPR and the DPA and must demonstrate that compliance by having in place appropriate technical and organisational measures to meet the requirements of accountability.

6. Processes for sharing

When information is shared, the sharing should be conducted in the most appropriate manner at that time and in accordance with the principles of the UK GDPR and the DPA.

The ways in which information may be shared are likely to include: verbally (eg meetings or telephone), in hard copy (eg reports, forms, printouts and other documents) or digitally (eg. secure email, access to IT systems where agreed, digital media, video-conferencing etc.)

7. Use of shared information

Any information shared under this ISA may only be used by:

- i) The OPCC for the purposes of the effective exercise of the PCC's statutory functions or as otherwise required by, or under, any rule of law.
- ii) TVP in the support of the PCC's or Chief Constable's functions, or for a policing purpose or as otherwise required by, or under, any rule of law.

There will be a presumption that any personal data will not be further disclosed by the receiving party without first consulting with the other party. At the time of sharing, the providing party may indicate that the personal data can be further disclosed subject to such conditions as may be determined. At the time of sharing, the providing party may stipulate that the personal data must not be further disclosed without the explicit prior written consent of the providing party (unless the receiving party is under a legal obligation to disclose the information).

As separate data controllers, both parties are individually obliged to ensure that information received from the other party which is personal data is processed in accordance with the requirements of the DPA and the UK GDPR.

8. Information Breaches

It is agreed that each party is responsible for their own breaches and that any breach made by an officer or employee of that party will be the subject of an internal inquiry; the party responsible for the breach to carry out a proportionate investigation in line with their own policies and procedures.

All breaches must be reported to the relevant Data Controller (being either TVP or the OPCC) within 24 hours of being made aware of a breach. If the data is jointly owned, the party responsible for the breach will be responsible for reporting that breach, however the other party should also be made aware of the breach as soon as possible. Both parties will provide reasonable assistance to the other when handling a data breach and each have a process and/or policy in place on how the reporting and investigation of breaches is to be managed.

In the event of action in respect of a data breach being brought by a data subject or the Information Commissioner's Office (the ICO), concerning the processing of shared personal data, against either one or both parties, each party will inform the other about any such action and will cooperate with a view to settling them amicably and in a timely fashion.

Persons to be contacted in the event of a Personal Data Security Breach:

TVP- Information Governance Team

InformationGovernanceTeam@thamesvalley.police.uk

OPCC- Data Protection Officer

Vicki.waskett@thamesvalley.police.uk

Deputy Data Protection Officer

Sierra.reid@thamesvalley.police.uk

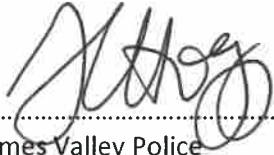
9. Miscellaneous Matters

Both parties:

- Agree that this ISA will come into effect on the date of the final signature below.
- Agree that they may withdraw from the ISA upon giving written notice to the other party. A party who withdraws must continue to comply with the terms of this ISA in respect of any information previously provided by the other party. Information which is no longer relevant should be returned or destroyed in an appropriate manner.
- Notwithstanding the above, in any event a party who withdraws from the ISA must continue to comply with the requirements of the PRSRA and the Policing Protocol.
- Agree to review the ISA every two years. The review will be initiated by either of the departments listed in section 4. They will consider whether the ISA is still useful and fit for purpose, identify any emerging issues, and recommend whether the ISA should be extended for a further period or terminated.
- Agree to ensure compliance with any handling requirements, for example those arising from the use of the Government Security Classification (GSC).
- Agree to ensure that the appropriate safeguards are in place in respect of the security of shared information and as to the individuals who may have access to it.
- Agree that should they receive any request for information, (for example a Freedom of Information request, Data Protection Right of Access request) that includes information provided by the other party they will consult the providing party, as soon as possible, and in any case prior to the disclosure of the information, in order that the potential implications of responding to the request can be fully assessed and any necessary remedial actions, such as redaction of data, initiated. In the event that a party proposes to provide or disclose information to a third party contrary to the wishes of the other party, they shall not do so without giving the other party reasonable written notice of their intentions and their reasons.
- Agree that should they receive any complaint concerning information provided by the other party they will advise the other party as soon as possible, and in any case prior to responding to the complaint.
- Agree to provide all staff involved with information sharing under this ISA with sufficient training and guidance to enable them to comply with this ISA.
- Agree that this ISA may be made available to the public in its entirety.

9. Signatories to this agreement

By signing this agreement, the parties acknowledge and accept the requirements placed upon them and others within their organisations by the agreement.



.....
Chief Constable of Thames Valley Police

Date Signed.....

07/08/23



.....
Police and Crime Commissioner for Thames Valley

Date Signed.....

7TH AUGUST 2023

