

# DATA SHARING AGREEMENT



Data Sharing Agreement (DSA)  
(hereafter referred to as The Agreement)

BETWEEN

SUSSEX POLICE (the Police)

AND

SUSSEX POLICE & CRIME COMMISSIONER (the Partner)

Version 3.1

This Agreement must not be circulated until approved by the Information Management team. Once approved, it will be returned to enable signatories to be collected and sharing to commence.

## **SECTION 1:**

1. Data Protection Impact Assessment (DPIA) questionnaire
2. Purpose
3. Statutory Powers to Process Personal Data
4. How / what information will be shared
5. Restrictions on information supplied.

## **SECTION 2:**

1. Agreement Overview
2. Introduction
3. Purpose
4. Partners
5. Statutory powers to process personal data
6. The Agreement
  - 6.1 Data quality
  - 6.2 Security and Audit
  - 6.3 Constraints on the use of information
  - 6.4 Review of the information sharing agreement
  - 6.5 Use of Microsoft Teams Chat Functions
7. Breaches
8. Data Subject Rights
9. Freedom of Information Act (FOIA) 2000
10. Signatories

## **SECTION 3:**

Police and Partner Signatures

## **SECTION 4:**

- Appendix A: Data Protection request forms and storage  
Appendix B: Email sharing and Government Security Classification (GSC)  
Appendix C: Information Governance Document  
Appendix D: Password Protection

**SUMMARY INFORMATION:**

<b>Date Agreement comes into force:</b>	31/10/2024
<b>Date Agreement review:</b>	31/10/2026
<b>Department Owning Agreement:</b>	Sussex Police Chief Constable
<b>Police Primary Contact:</b> (Name and Warrant / Fin / Pay Number)	CC Jo Shiner EA597
<b>Police Secondary Contact:</b> (Name and Warrant / Fin / Pay Number)	Carl Lovell 63488

**AGREEMENT TEMPLATE VERSION REVIEWS:**

<b>Version</b>	<b>Comments</b>	<b>Made By</b>
v1.0	<i>Initial Submission</i>	<i>05/11/2018 – UK GDPR compliant DSA approved and implemented.</i>
V2.0	<i>Annual review of V1 template, updated for 2019 onwards</i>	<i>01/05/2019 – Review and changes to template made by Information Management.</i>
V2.1	<i>Updated following ICO Law Enforcement Processing Guidance</i>	<i>01/02/2020 - Review and changes to template made by Information Management.</i>
V2.2	<i>Updated to change the format</i>	<i>04/02/2020 – Review by Sussex and Surrey IM Teams.</i>
V2.3	<i>Update based on audit of joint DSA process</i>	<i>01/06/2020 – Review by Information Management teams in line with National guidance and Audit review.</i>
V2.4	<i>Updates to Security &amp; Review in Section 1 and amendments to email addresses</i>	<i>11/05/2022 – Review by Information Governance Sussex</i>
V2.5	<i>Reviewed based on challenges from V2.4</i>	<i>28/09/2022 - Review by Information Governance Sussex</i>
V2.6	<i>Reviewed based on challenges from V2.5</i>	<i>15/08/2023 – Review by Information Governance Sussex</i>
V3.1	<i>DSA Reviewed by Sussex Information Governance team</i>	<i>17/06/2024 - Review by Information Governance Sussex</i>

**FORCE DATA PROTECTION OFFICER (DPO) AND POLICIES LINKS:**

**Sussex Police** DPO – Jim Collen  
[DPO@sussex.police.uk](mailto:DPO@sussex.police.uk)  
[Sussex Police Privacy Notices](#)  
[Data Protection Policy](#)

# SECTION 1

## 1. DATA PROTECTION IMPACT ASSESSMENT (DPIA) QUESTIONNAIRE

It is a mandatory requirement to assess the processing of an individual's personal data using a DPIA to ensure all risks surrounding the processing have been assessed. All Agreements must be accompanied by the questions below.

### Processing of Data Under This DSA:

How will you share the data, what process(es) will be used?
<i>Data will be shared when required and this will be done via secure email or verbally</i>
Will you be sharing digital media, such as BWV, CCTV, etc?
<i>If it is relevant and proportionate to do so</i>
Will individuals be aware that we are sharing their data in this way?
<i>No</i>
Will access to the data be restricted / limited to specific users?
<i>Yes, Sussex Police and OSPCC</i>
Is this a new process or an updated one?
<i>This is a refreshed agreement in relation to an already existing process</i>
What / who is the source of the data for the signatory agencies (offenders, victims, etc)?
<i>This could be in relation to victims, offenders, witnesses, or any person linked to a Sussex Police case or investigation</i>
Will signatory agencies process sensitive / special category personal data such as race, religion, medical, etc?
<i>There is a potential for this to be shared however, it depends on the circumstances and whether is relevant or proportionate to do so</i>
Will signatory agencies on the DSA process details on children or other vulnerable people?
<i>Potentially, data will be shared in relation to children and / or vulnerable adults</i>
How often will signatory agencies capture / share the data, weekly, monthly, real time, etc?
<i>Data will be shared as and when required</i>
Have you considered and complied with any relevant Codes of Practice (if so, please list)?
<i>Yes, in accordance with the legislation laid out in Section 1 (3)(i) of this DSA</i>
Do any external Partners or suppliers have direct or indirect access to Police systems?
<i>No</i>
Will the project involve automated decision making about an individual?
<i>No</i>
Will any data be transferred outside of the UK?
<i>No</i>
Are any of the signatory agencies or their processors located outside of the UK?
<i>No</i>

### Signatory Agency Processing:

	Police	Signatory Agency
Is there automated / manual deletion of data on signatory agencies systems?	There is a Retain, Review Delete (RRD) function within NICHE	There is a retain, review and delete function available within Caseworker.
What are the retention periods for any shared data?	Retention periods fall in line with Management of Police Information (MoPI).	The OSPCC has a Disposal and Retention Schedule to manage all information held.
Can data be audited? If so, by whom?	Data is fully auditable by PSD.	Data is fully auditable by the Senior Management Team within the OSPCC.
How and where will signatory agencies store the data?	Police will store any data shared, either in NICHE or SharePoint.	The OSPCC will store any data shared either in Caseworker or on the shared drive.
Can data be edited by signatory agencies if found to be inaccurate?	NICHE and SharePoint are both editable.	Caseworker and the shared drive are both editable.
Does this leave an audit trail?	NICHE and SharePoint have a robust audit trail.	Caseworker and the shared drive both leave an audit trail.

How long will signatory agencies store the data?	Data will be stored in line with MoPI.	Data will be stored in line with the Disposal and Retention Schedule for the OSPCC.
--	--	---

## PURPOSE

- i. The information can only be shared for the purpose described in this Agreement and where there is a legal basis for sharing the information.
- ii. The purpose of this Agreement is to facilitate the lawful sharing, use and security of personal, special / sensitive category and criminal offence data to safeguard those who require safeguarding intervention and to facilitate the relevant statutory functions.
- iii. This Agreement will function as the foundation to embed strong, effective multi-agency arrangements that are responsive to local circumstances and engage the right people.
- iv. No information shall be disclosed without a legal basis for doing so. All disclosures must comply with the signatories' legal obligation under the UK Data Protection Legislation.
- v. 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.
- vi. The Purpose of this Agreement is outlined below:
  - To assist the OSPCC in exercising his/her statutory functions.
  - Is to ensure that sharing would not prejudice any ongoing or potential investigations or prosecutions by Sussex Police or other parties.
  - To ensure that sharing would not contradict any legal obligation upon Sussex Police that prohibits or precludes sharing.

## 2. STATUTORY POWERS TO PROCESS PERSONAL DATA

- i. The principal legislative (including Act and Section) instruments that provide powers to lawfully share information under this Agreement are:

### **Policing Protocol Order 2011**

19. In order to enable the OSPCC 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 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.

21. Information will be shared by the OSPCC with Sussex Police where necessary to exercise theirs or Chief Constable's functions or where necessary for a policing purpose. The Chief Constable is responsible to the public and accountable to the OSPCC for providing them with access to information, officers and staff as required.

23 (e) providing the OSPCC with access to information, officers and staff as required.

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

- ii. Before the Police can share information, a lawful basis for sharing personal and special category / sensitive information (including distinction between employment and law enforcement purposes) must be identified and detailed in this Agreement.
- iii. Partners Lawful basis for processing Personal Data Article 6 (1) UK GDPR. Where personal data processing under this agreement falls outside of the law enforcement purposes, processing must still be necessary for a wider policing purpose.
  - (c) Legal obligation: processing is necessary for you to comply with the law (not including contractual obligations).
  - (e) Public task: 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.

- iv. Partners Lawful basis for processing Special Category Data Article 9 (2) UK GDPR. Where personal data processing under this agreement falls outside of the law enforcement purposes, processing must still be necessary for a wider policing purpose.
- (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
  - (g) processing is necessary for reasons of substantial public interest (see below for the conditions), 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 the interests of the data subject.
- Statutory and government purposes
  - Administration of justice and parliamentary purposes
  - Equality of opportunity or treatment
  - Racial and ethnic diversity at senior levels
  - Preventing or detecting unlawful acts
  - Protecting the public
  - Regulatory requirements
- v. Police Lawful basis for processing sensitive data for DPA 2018, Part 3 Law Enforcement Purpose. It is understood that most of the personal data processing undertaken under the remit of this agreement will fall under Data Protection Act 2018, Part 3, Law Enforcement Processing.
- vi. For the purposes of this Agreement, the Police will share Personal / Sensitive Data under Police's statutory functions and where processing is necessary for the performance of a task carried out for that purpose by a competent authority. The definition of statutory function for 'law enforcement purposes' is 'purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
- vii. In addition, the police will share Sensitive data where the processing is strictly necessary for the law enforcement purpose and the processing meets at least one of the conditions in Schedule 8, Part 3 DPA 2018 namely:
- Judicial and statutory purposes/administration of justice
  - Legal claims and judicial acts
- viii. Partner signatories to this agreement are **Processors** in relation to the data shared under this agreement.

### 3. HOW / WHAT INFORMATION WILL BE SHARED

- i. The Police will share:
- The sharing would not prejudice ongoing or potential investigations or prosecutions by Sussex Police or other parties.
  - The sharing would not contradict any legal obligation upon Sussex Police that prohibits or precludes sharing.
- ii. The OSPCC will share:
- Information will be shared by the OSPCC with Sussex Police where necessary to exercise theirs, or Chief Constable's functions or where necessary for a policing purpose.
  - The sharing is reasonably required by the OSPCC to assist them in exercising his/her statutory functions.
  - Both individuals will be responsible for the management of this ISA and ensuring compliance with it.
  - They will be responsible for the initial revision of this ISA.
  - Information will be shared by the OSPCC with Sussex Police where necessary to exercise theirs or Chief Constable's functions or where necessary for a policing purpose.

This ISA is not intended to cover:

- Information sharing between the OSPCC and the Sussex Police & Crime Panel.
- Information sharing between the Chief Constable of Sussex Police and the Sussex Police & Crime Panel.

- iii. This information will be shared verbally and via secure email.

#### 4. RESTRICTIONS ON INFORMATION SUPPLIED

- i. All shared data will be held in line with the organisation's retention schedule or until no longer operationally required.
- ii. Information shared under this Agreement will be securely stored and disposed of when no longer required for the purpose for which it is provided unless further retention is justified as lawful.
- iii. Police files containing information from Partners will be reviewed and deleted in line with Force policy and the Force retention schedule.
- iv. If you are transferring data outside the UK, then you must record the measures that the organisation receiving the personal data has taken to provide adequate safeguards.
- v. Information shared by the Police is classified as OFFICIAL – SENSITIVE and comes with clearly marked handling instructions. Any improper disclosure, copying, distribution or use of this information is prohibited, and any subsequent personal data breach will be the responsibility of the signatory agency.
- vi. The sharing partner(s) are Data Controller of any shared documents throughout their lifecycle. Only a verbal disclosure of this document can be given to Professionals and Family, under no circumstances is an un-redacted copy to be shared without permission.
- vii. Any requests from Data Subjects to exercise their Rights of Access (ROA) for Police shared information must be referred to Sussex Police for review and disclosure. Data subjects should be directed to the [Sussex Police website](#) to make a request.
- viii. Similarly, any ROA requests received by Sussex Police will be directed to the relevant Partner to review and respond.
- ix. Under no circumstances is the image to be printed and displayed in a private area. The image is to be retained as digital only, and only further shared through secure and approved platforms. This does not include further dissemination through the use of WhatsApp and other social media.

## SECTION 2:

### 1. AGREEMENT OVERVIEW

- i. The following Data Protection legislation impacts on the sharing requirements for this Agreement:
  - The UK General Data Protection Regulation (UK GDPR) 2018
  - The Data Protection Act 2018
  - Privacy and Electronic Communications Regulations 2019

### 2. INTRODUCTION

- i. The Police are committed to partnership working and are continually looking for opportunities to enhance professional working practices.
- ii. This Agreement outlines the need for the Partners to work together to share information in line with the Policing Purposes as set out in the Management of Police Information Code of Practice. The Policing Purposes are described as:
  - Protecting life and property.
  - Preserving order.
  - Preventing the commission of offences.
  - Bringing offender to justice and
  - Any duty or responsibility arising from common or statute law.
- iii. This Agreement ensures information is processed lawfully and determines the roles and responsibilities of each organisation to ensure the sharing is accurate, necessary, proportionate, and lawful.

- iv. The Police are committed to tackling Crime and Disorder and supporting Public Protection in collaboration with members of this Agreement.
- v. The purpose of this document is to enable routine and effective information sharing between the Partners. It will incorporate measures aimed at:
  - Facilitating a coordinated approach that targets crime and anti-social behaviour and supports and enables public protection (safeguarding).
  - Facilitating the collection and exchange of relevant information
  - Ensuring that the sharing of information meets one or more of the policing purposes.
  - Where appropriate, supporting the pursuit of criminal or civil proceedings.
- vi. It is the responsibility of each Partner to ensure:
  - Information is shared securely with the point of contact.
  - The information shared is documented by the owning organisation.
  - Information is shared only on a 'need to know' and with a legal basis.
  - There are clear procedures to be followed regarding information sharing.
  - Information will only be used for the reason(s) it has been obtained.
- vii. This Agreement will clarify any specific arrangements.
- viii. Sharing within this Agreement is covered by [UK Data Protection Legislation](#) and all applicable laws and regulations relating to the processing of personal data and privacy (including guidance issued by the Information Commissioners 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.
- ix. It is the responsibility of all Partners to ensure that all information shared is:
  - as a minimum, that the date, time, and summary of the data shared is recorded (ideally copies of data shared should be retained, especially if amended / sanitised)
  - a mechanism exists by which the flow and integrity of information can be controlled.
  - appropriate training on this agreement and the Data Protection legislation (DPA 2018) and UK GDPR is given to all relevant staff.
  - adequate arrangements exist to test adherence to the Agreement.
  - sharing is covered under each Partners Privacy Notice (must be available on request)
  - each partner's Data Protection Policy is made available to all partners (must be available on request)
- x. Neither Partner shall be liable or accept liability in respect of actions, proceedings, or penalty by a data subject or the ICO following the use or possession of the Shared Personal Data (including special category / sensitive data).
- xi. Partners undertake to have in place throughout the term of this agreement, appropriate technical and organisational security measures to prevent unauthorised or unlawful processing of the shared personal data, including accidental loss or destruction.

### **3. PURPOSE**

- i. This Agreement sets out the framework for sharing personal data between the Partners. It defines the principles and procedures that shall be adhered to and the responsibilities between Partners.

### **4. PARTNERS**

- i. Details of all Partners, including their name and address and ICO registration number (if applicable), will be provided on request.

### **5. STATUTORY POWERS TO PROCESS PERSONAL DATA**

- i. The principal legislative instruments that provide powers to lawfully share information under this Agreement are detailed in Section 1, Paragraph 3.
- ii. Police Part 3 Processing: Any Information sharing under this agreement for the law enforcement purpose will comply with the Data Protection Principles set out in DPA 2018 Sections 29, 32, 40, Schedule 2 and Schedule 8.

- iii. All Information Sharing Agreements will be compliant with the European Convention of Human Rights and the Human Rights Act 1998, in particular, Article 8 of the Convention.
- 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. Personal data shall be processed fairly, in a transparent manner and lawfully and in particular, shall not be processed unless at least one of the lawful basis for processing exists under Article 6 of the UK GDPR.
- vi. Data shall be processed fairly, in a transparent manner and lawfully and in particular, shall not be processed unless at least one of the lawful basis for processing exists under Article 6 of the UK GDPR and a separate condition for processing special category data under Article 9 is met.
- vii. Personal data relating to criminal convictions and offences or related security measures shall be processed fairly, in a transparent manner and lawfully and in particular, shall not be processed unless at least one of the lawful basis for processing exists under Article 6 of the UK GDPR and a separate condition for processing special category data under Article 9 is met and shall comply with Article 10 and only be carried out only under the control of official authority.
- viii. Transferring sensitive personal data from Part 3 (Law Enforcement Purpose) to Part 2 (General Processing): Personal data, including Sensitive Data will only be transferred from DPA 2018 Part 3 into DPA 2018 Part 2 processing where a condition in DPA 2018 Schedule 8 is met. The data will then be processed as special category data where the requirements and conditions are met. See Section 2, Paragraph 3.

## 6. THE AGREEMENT

- i. This Agreement facilitates 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. This Agreement is not contractually binding but is setting good practice standards that the sharing partners are required to meet.
- iii. Information sharing within the community is undertaken to remove or minimise discriminatory practices. This includes where victimisation is based on characteristics such as race, sex, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership and gender reassignment.
- iv. It is incumbent that all staff regularly assess their information sharing activities and monitor any impacts to ensure compliance with the Equality Act 2010. We should not disclose personal information about an individual's identity unless we have their permission to do so, or the disclosure is necessary for the purpose of preventing or investigating crime. It is essential that all disclosures falling under the Gender Recognition Act are thoroughly assessed before being shared to ensure the individual's privacy is respected. For further assistance, please see section 22 of the Gender Recognition Act, which offers protection to people who possess a Gender Recognition Certificate (GRC). Not everyone who identifies under the 'trans umbrella' will have a GRC, but it is still essential that their privacy is protected. The Data Protection Act and organisational Codes of Ethics, or similar, will offer protection to those people who do not hold a GRC.
- v. This Agreement applies to any personal or confidential information, irrespective of the medium in which it is held e.g. paper based, electronic (including the cloud), 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.
- vi. 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.
- vii. It is the responsibility of each signatory to ensure that:
  - Information shared is in accordance with the law.
  - Appropriate staff training and awareness are provided to your staff in relation to Data Protection, including information sharing and the processing outlined under Section 1 of this Agreement.
  - Information is shared responsibly securely 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. (see Appendix A Data Protection Request Form and Storage)
  - Information shared under this agreement will be appropriately marked under the Government Security Classification (GSC) and have handling conditions applied where necessary (see Appendix B (Email Sharing and GSC). This is necessary to maintain the security of the data shared between signatories.
  - Replies may be communicated via e-mail should the recipient subscribe to an encrypted / secure email server (see Appendix B (Encrypted Emails - Secure Domain Email Addresses) for guidance).
  - Bulk / Special Category / Sensitive Data can be provided via email if they are encrypted for Force minimum standards (see Appendix D for guidance).
- viii. 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.
- ix. If you are transferring data outside the EEA, then you must record the measures that the organisation receiving the personal data has taken to provide adequate safeguards under the UK Data Protection Legislation.
- x. The Police utilise a business analytics tool that provides interactive, accessible, visually immersive, and easy to interpret data using multiple sources. This data pooling will be proportionate and for specific purposes.
- xi. Any Partners named in this document may terminate their involvement at any time. They must inform all the single points of contact, who in turn will inform their relevant Information Governance Manager.

- xii. Any Partner may make suggestions for amendments to the agreement at any time in consultation with Sussex Police Information Management team.

## **6.1 DATA QUALITY**

- i. It is the responsibility of all Partners to ensure that the information is of sufficient quality for its intended purpose, bearing in mind accuracy, validity, reliability, timeliness, relevance, and completeness.
- ii. The Police will take every reasonable step to ensure that inaccurate personal data is erased or rectified without delay and will notify the Partners to this agreement of the erasure or rectification.
- iii. If a Partner decides to erase or rectify personal data, it is their responsibility to contact all Partners that have received the relevant data as soon as possible.

## **6.2 SECURITY AND AUDIT**

- i. Partners of this agreement will implement information security measures suitable for the type and sensitivity of the data being processed. Partners are at liberty to request copies of each other's:
  - Information Security Policy
  - Records/Information Management Policy
  - Data Protection Policy
- ii. Signatories may exercise their right under this Agreement to audit compliance in relation to its shared information. This will require the signatories to evidence data protection compliance and to provide details of any further processing of specific personal / special category / sensitive information.
- iii. Signatories need to ensure sufficient technical processes are in place to protect their systems and the data held within from cyber-attacks.

## **6.3 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 Partner 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. The Partners shall not assign, sub-contract or transfer its rights or obligations under this Agreement in whole or part to any third Partner without prior written consent of the other Partners.
- 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.

#### 6.4 USE OF MICROSOFT SHAREPOINT AND TEAMS CHAT FUNCTION

- i. Only relevant / necessary / proportionate information should be freely shared within the Teams channel (removing the need for the DP2 form). All shared information must be perceived as Official Sensitive and carry handling conditions as below:
  - *The information in this document is for the **exclusive** use of **the partner agency with whom it has been directly shared**.*
  - *This information must not be passed on to any third party without the express written permission of the Data Controller.*
  - *This information must be kept secure and securely disposed of when no longer required for its original purpose.*
  - *Be aware that any **improper disclosure, copying, distribution or use** of the contents of this information is **prohibited** and **criminal proceedings** may follow.*
- ii. When sharing personal information, agencies must retain an audit record, including:
  - *The information shared.*
  - *The reason for the request/sharing*
  - *What was the legitimate purpose, i.e. Prevent / Detect Crime etc.*
- iii. Proportionality must be applied by the owning partner before any data is shared and then further restricted to only specific / relevant partners. Partners will be responsible for any necessary redactions prior to sharing on this platform.
- iv. The information could be in relation to any person who has involvement with these services, this can include children who are involved with the services.
- v. Further guidance can be found in the appendices section under Appendix C: Information Governance Document.
- vi. The Sussex Police default expiration date for 'Teams Chats' and files relating is 2 years. Whilst there is an expiry time, two years in Sussex Police, this is not to be regarded as a case management system but as a conduit to share information.
- vii. The Sussex Police default expiration date for 'Teams meeting recordings' is 60 days. When meetings are scheduled from Outlook or Teams calendar, recordings are automatically stored in OneDrive > Recordings folder. When meetings are scheduled from Teams/channels, Sussex Police recordings are stored on SharePoint Online. There is an option to extend the expiration date in Teams settings.

#### 6.5 REVIEW OF THE AGREEMENT

- i. This Agreement will be reviewed 12 months after its implementation and every two years thereafter.
- ii. Any changes will be signed and verified by Information Management and the Agreement may be published on the Police websites.
- iii. Signatories of this Agreement may undertake checks with Partners to ensure sharing is compliant with the processes and constraints stipulated within this agreement.

#### 7. 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. The Partners shall each comply with its obligation to report a personal data breach to the appropriate supervisory authority and (where applicable) data subjects under UK Data Protection Legislation. Partners shall each inform the other Partner of any personal data breach irrespective of whether there is a requirement to notify any supervisory authority or data subject(s).
- iii. 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.

- iv. The Partners 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 Partners, the Partners will inform each other about any such disputes or claims and will cooperate with a view to settling them amicably in a timely fashion.
- v. Partners undertake to ensure that any use or reuse of the data disclosed is lawful, compliant with the data protection principles and processed using appropriate safeguards to the rights and freedoms of the data subject.
- vi. Breaches of this Agreement will lead to a review and possible termination of this Agreement (including the destruction of all previously shared information).

## **8. DATA SUBJECT RIGHTS**

- i. Each signatory (controller) is responsible for responding to the information that they own in relation to [subject rights requests](#) (including access, erasure, rectification, restriction of processing and objection to processing).
- ii. Each signatory (controller) will inform the Partners Data Protection Officer (DPO) within 2 working days of any changes made through rights of erasure, restriction, or rectification.

## **9. FREEDOM OF INFORMATION ACT (FOIA) 2000**

- i. All FOI requests will be managed in accordance with the FOIA and / or Environmental Information Regulations
- ii. Any FOI requests will be passed to the owning Partner within 2 working days to enable compliance (Section 10 of the FOIA or Regulation 5 of the Environmental Information Regulations).
- iii. In the interests of transparency, and to assist in meeting the fairness principle, Partners may publish this agreement on their website. Where this is not felt appropriate the rationale and any exemptions being claimed should be recorded internally.

## **10. SIGNATORIES**

- i. All agencies that are part of the information sharing process will be, upon signing this Agreement, bound to comply with its terms.
- ii. 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.
- iii. Where a signatory leaves the organisation, it is not a requirement to re-sign the Agreement. However, the details of the new SPoC must be circulated in writing to all Partners.
- iv. Whilst the DSA is out with Partners for review, the existing Agreement can continue to be used until the revised / updated version is issued. This extension is for a period of 28 days maximum.

## SECTION 3 – 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. Any signatory to this Agreement may withdraw on giving written notice to the other Partners. The withdrawing Partner will be bound to comply with those relevant terms of this Agreement, which remain effective following withdrawal.
- iii. Where the Chief Executive or Director of a Partner leaves the organisation, it is not a requirement for that Partners to re-sign the Agreement.
- iv. If a signatory changes, contact details of the new SPoC must be circulated in writing to all other Partners.
- v. I hereby agree that the information in this document is correct and confirm that my electronic signature authenticates this Agreement.

### Police Primary Contact:

Full Name	Joanne Shiner	
Warrant / Pay / Fin	EA579	
Email Address	<a href="mailto:jo.shiner@sussex.police.uk">jo.shiner@sussex.police.uk</a>	
Role and Rank	Chief Constable	
Date of Signature	06/12/24	

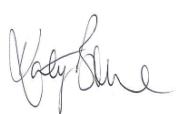
### Agreement approved for circulation by Information Governance:

Full Name	Carl Lovell
Warrant / Pay / Fin	63488
Email Address	<a href="mailto:carl.lovell@sussex.police.uk">carl.lovell@sussex.police.uk</a>
Role and Rank	Information Governance Supervisor
Date of Signature	05/12/2024

### Partner Agency Signatories:

I, the undersigned, on behalf of my organisation, agree to this Information Sharing Agreement.

### Partner Organisation      OSPCC

Full Name	Katy Bourne	
Job Title	Sussex Police & Crime Commissioner	
Email Address	<a href="mailto:katy.bourne@sussex-pcc.gov.uk">katy.bourne@sussex-pcc.gov.uk</a>	
Date of Signature	10/12/2024	
Privacy Notice Link	<a href="https://www.sussex-pcc.gov.uk/media/8545/privacy-notice-for-the-ospcc-march-2024.pdf">https://www.sussex-pcc.gov.uk/media/8545/privacy-notice-for-the-ospcc-march-2024.pdf</a>	
Data Protection Policy Link	<a href="https://www.sussex-pcc.gov.uk/about/how-we-work/data-protection/">https://www.sussex-pcc.gov.uk/about/how-we-work/data-protection/</a>	

# SECTION 4 – APPENDICES

## APPENDIX A: DATA PROTECTION REQUEST FORMS AND STORAGE



ISA Doc -Data  
Protection Request Fo

## APPENDIX B: EMAIL SHARING AND GSC



Email Sharing and  
GSC.docx

## APPENDIX C: INFORMATION GOVERNANCE DOCUMENT



Information\_Governance\_Document\_V1.2.d

## APPENDIX D: PASSWORD PROTECTION



Password\_Protection\_  
Word.docx