



# Wales Accord on the Sharing of Personal Information

## Information Sharing Protocol for Community Safety Partnership

**Version** 1.0

Date Assured 24.07.2024

Quality Assurance Group South Wales

## Contents

1	Introduction to this ISP	2
2	The information sharing partner organisations	2
3	Specific organisational / practitioner obligations	4
4	Legislative / statutory powers	4
5	Personal information to be shared	8
6	Data Subjects' Rights	9
7	Information security	12
8	Review, Breaches and Termination of this Agreement	12
9	Appendix A – Glossary of Terms	13
10	Appendix B – Information Reference Table	15

## 1 Introduction to this ISP

- 1.1 This Information Sharing Protocol (ISP) is supplementary to the Wales Accord on the Sharing of Personal Information (WASPI) and has been agreed following consultation between the participating partner organisations.
- 1.2 This ISP is intended to help practitioners understand what information can be shared between the listed partners for the stated purpose(s). It also provides assurance that the partners have considered the requirements of data protection legislation.
- 1.3 This ISP has been prepared to support the regular sharing of personal information between Cardiff's Community Safety Partnership noted organisations. The Partnership is a collaborative effort which aims to enhance the ability to detect and prevent crime and anti-social behaviour, in addition to addressing matters of significant public interest.
- 1.4 Personal information is shared for the purpose of accurately identifying core issues that may stem from crime, deprivation, poverty, and cultural trends.

This ISP supports the delivery of the Partnership by ensuring more effective joint working and enabling the delivery of multi-agency work, key priorities, strategy, and policy development. Through the exchange of crime data, anti-social behaviour data, and council owned data (detailed in Appendix B), members will have a greater ability to prevent and/or detect crime and anti-social behaviour concerns of public interest, and to work together to address issues or to tailor interventions accordingly.

The Community Safety Partnership aims to ensure the safety and well-being of the local community. Cardiff Council's Community Safety Team are responsible for acting on the Public Service Board's behalf to address various safety issues, supporting vulnerable individuals, and to foster a sense of security within the community. The team also works on initiatives to reduce anti-social behaviour, respond to incidents, and engage with residents to address their safety concerns.

## 2 The information sharing partner organisations

- 2.1 The table below sets out the organisational partners to the ISP, the key contact points and the departments, divisions and teams typically involved in sharing information for the purposes described in this ISP.

Information Sharing Partner Organisations	Owner / Point of contact	Departments / Divisions / Teams
Cardiff Council	Community Safety Project Manager Senior Partnership Analyst	Community Safety
	Antisocial Behaviour Manager Service Manager for supported Accommodation	Housing & Communities
	Senior Policy Officer	SAFE Partnership
	Senior Collections & Cleansing Officer	Recycling & Neighbourhood Services
	Project Manager	Youth Justice Services
	Education Welfare Manager	Education/Emotional Health and Wellbeing Service

	Parks Manager	Parks and Recreation
	Community Engagement Manager	Ask Cardiff
	CCTV Manager	CCTV
	Child Friendly Coordinator	Child Friendly City
	Social Workers	Children and Adult Services
South Wales Police	Community Safety Manager Intelligence Analysts Cardiff Neighbourhood Policing Team	Community Safety
British Transport Police	Analyst Command Team	Cardiff Team
Shared Regulatory Services	Operational Manager Shared Regulatory Services	Commercial Services and Trading Standards/ Wales Illegal Money Lending Unit (WILMLU)
South Wales Fire & Rescue Services	Fire Crime Practitioner Fire Crime Unit Analyst	South Wales Fires and Rescue Cardiff
Cardiff and Vale University Health Board	Harm Reduction Lead/ Commissioning Manager for Substance Misuse & Harm Reduction Violence Prevention Nurses Team Substance Misuse, Harm Reduction & Safeguarding Service Lead Head of Safeguarding Alcohol Treatment Centre Team	Commissioning of Services  Accident and Emergency  CAVDAS - Cardiff & Vale Drug and Alcohol Services  Safeguarding  Alcohol Treatment Centre (ATC)
Welsh Ambulance Service Team (WAST)	Information Analyst	Health Informatics Department
His Majesty's Prison and Probation Service	Head of Probation Delivery Unit & Deputy Head of Probation Delivery Unit	Cardiff Delivery Unit
Action for Children	Service Manager	Sidestep Cardiff
South Wales Victim Support	Victim Support Officer	Local Team
Crimestoppers	Fearless Outreach Worker	Local Team
Safer Wales	Director of Project Development	Local Team
FOR Cardiff	Evening and Night Time Economy Manager/ Projects Manager	Business Improvement
Vinci	Project Manager	Vinci Facilities

- 
- 2.2 The ISP owners / points of contact have overall responsibility for this ISP within their respective organisations and must therefore ensure the ISP is disseminated, understood and acted upon by relevant practitioners.
  - 2.3 The owners / point of contact for each partner organisation will regularly monitor and review the use of this ISP to ensure information is shared effectively and appropriately.
  - 2.4 Once the ISP has been assured, each partner organisation will nominate a signatory to sign the ISP at Appendix C. The signatory will be an appropriate person from the partner organisation who can sign on behalf of the organisation.

### **3 Specific organisational / practitioner obligations**

- 3.1 Any breaches of security, confidentiality and other violations of this ISP must be reported in line with each partner organisation's incident reporting procedures. Consideration should be given to sharing the outcome of any investigation, where appropriate, with other partners to the ISP.
- 3.2 Practitioners who share information in line with this ISP should make themselves aware of, and adhere to, their organisation's Information Governance and records management procedures; in particular the provisions that relate to collecting, processing and disclosing personal information.
- 3.3 Every reasonable step should be taken to ensure that inaccurate personal data are erased or rectified without delay. Consideration must be given to advising partner organisations that they may have received inaccurate information. In circumstances where partner organisations cannot be informed, advice should be taken from an Information Governance lead (or equivalent).

### **4 Legislative / statutory powers**

**STAFF SHOULD NOT HESITATE TO SHARE PERSONAL INFORMATION IN ORDER TO PREVENT ABUSE OR SERIOUS HARM, IN AN EMERGENCY OR IN LIFE-OR-DEATH SITUATIONS.**

**IF THERE ARE CONCERNS RELATING TO CHILD OR ADULT PROTECTION ISSUES, THE RELEVANT ORGANISATIONAL PROCEDURES MUST BE FOLLOWED**

- 4.1 The sharing arrangements described in this ISP takes into account the relevant data protection legislation, the Human Rights Act 1998 and the common law duty of confidence.
- 4.2 Before sharing personal information, partner organisations must have identified a clear legal basis for doing so.
- 4.3 Data protection legislation includes the concept of:
  - **'personal data'**; any information relating to an identified or identifiable (living) natural person, and
  - **'special categories of data' / 'sensitive processing'**; personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

---

Whilst information about deceased people is not covered by data protection legislation, data about deceased people is covered by a similar level of confidence.

- 4.4 Further information and guidance on lawful processing of personal information can be found on the Information Commissioner’s website; [www.ico.org.uk](http://www.ico.org.uk)
- 4.5 Partner organisations also need to ensure they take into account the Data Protection Act 2018 and any additional requirements it places on the use of the legal bases set out in Articles 6, 9 and 10 of UK GDPR (see Part 2 of the Act) and processing for the ‘law enforcement purposes’ (see Part 3 of the Act). The ICO has guidance on this matter and queries about the relevance of any legal basis should be raised with an Information Governance lead.
- 4.6 Consent to process personal data should not be confused with consent to receive the service. The two are separate and should not be confused or merged.

### HOW TO USE THE TABLES

The following tables are designed to allow partners to this agreement to highlight the lawful bases relevant to the sharing described in this ISP. Please consider the guidance below, and take advice from your Data Protection Officer or equivalent. Definitions of terms can be found at Appendix A.

#### **TABLES 1 & 2 – personal data and special categories of personal data**

In most cases, information sharing partners will need to:

- Select at least one lawful basis from table 1 (sharing personal data), **and**
- Select at least one lawful basis from table 2 (processing special categories of data).

Notes: Usually, only one lawful basis should be selected in table 1 and one in table 2. If more than one lawful basis is selected in either table (for example if partner organisations are relying on different lawful bases), please add an explanatory note.

#### **TABLE 3 – personal data about criminal convictions, offences etc.**

- The lawful basis for sharing personal data about criminal convictions, offences or related security measures should be recorded in table 3.
- You **will always** have to complete table 1.
- If you are sharing special categories of personal data, you will also have to complete table 2.

#### **TABLE 4 – processing by competent authorities for law enforcement purposes** (as defined by Part 3 of the Data Protection Act 2018).

- Complete table 4 only if personal data is being processed by competent authorities **and** only for law enforcement purposes.
- If information is being shared for law enforcement and other purposes you may also need to complete tables 1, 2 & 3.

### Table 1 - Article 6 - Personal Data

Legal basis	Check box / Notes
Task carried out in the public interest or in the exercise of official authority – Art 6(1)(e)	<input checked="" type="checkbox"/> <p>Community Safety Partnerships (CSPs) are an important feature of the network of partnerships that help to tackle crime and reduce reoffending and were set up under <b>Sections 5-7</b> of the Crime &amp; Disorder Act 1998. There are about 300 CSPs in England and 22 in Wales usually at district or unitary authority level and are made up of representatives from Police, Probation Service, Local Authority, Health, Fire and Rescue authorities. By extension, <b>Section 17</b> details the Local Authority's duty to consider Crime and Disorder Reduction while exercising their various functions.</p> <p><b>The lawful basis for public authority partners is public task Art 6 (1) (e).</b></p> <p><b>Section 115</b> of the Crime and Disorder Act 1998 gives partners the power to share information for the purpose of reducing crime and disorder. Schedule 9 (5) of the Police and Justice Act strengthens this by introducing a new duty on the same agencies. Additionally, anti-social behaviour and other behaviours which adversely affect the local environment are here included under the scope of 'Crime and Disorder'.</p>
Necessary for compliance with a legal obligation – Art 6(1)(c)	[Organisations must be able to identify the specific legal obligation that requires information to be shared and should include the details here – title of legislation and relevant section(s)]
Legitimate Interest – Art 6(1)(f)	<input checked="" type="checkbox"/> <b>Third party partners will rely on legitimate interest to process personal data.</b>

**Table 2 - Article 9 - Special Categories of Personal Data**

Legal basis	4.7 Checkbox / Notes
Necessary for reasons of substantial public interest - Art 9(2)(g)	<input checked="" type="checkbox"/> <p>UK GDPR Art 9(2)(g) requires a basis in UK law, which is provided by Section 10(3) of the Data Protection Act 2018.</p>

	<p>This in turn refers to the need to meet a relevant condition in Part 2 of Schedule 1 of the DPA 2018. The relevant condition is:</p> <p>Preventing or detecting unlawful acts 10(1) -</p> <p>(a) is necessary for the purposes of the prevention or detection of an unlawful act.</p> <p>(c) is necessary for reasons of substantial public interest.</p> <p><i>Most of these Schedule 1 conditions also require an Appropriate Policy Document, each organisation should meet this requirement prior to sharing.]</i></p>
Legitimate Activities – Art 9 (2)(d)	[This legal basis should only be relied upon by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and the processing relates solely to members, former members, persons who have regular contract with it and the personal data is not disclosed outside of the body without consent of the data subjects]
Provision of preventative or occupational medicine, health or social care or treatment, or the management of health or social care systems – Art 9(2)(h)	<input type="checkbox"/>

**Table 3 - Article 10 - Personal Data about criminal convictions, offences or related security measures**

The sharing of personal data relating to criminal convictions, offences, or related security measures	<p>Processing is:</p> <p><input checked="" type="checkbox"/> Carried out under the control of an official authority / competent authority</p> <p>_____ and/or _____</p>
	<p><input checked="" type="checkbox"/> Meets a relevant condition in Part 1, 2 or 3 of Schedule 1 of the Data Protection Act 2018. The relevant condition is: Part 2 Art 10(1)</p> <p>(a) - necessary for the purposes of the prevention or detection of an unlawful act and (c) is necessary for reasons of substantial public interest.</p>

**Table 4 - Competent authorities for Law Enforcement Purposes**

Processing <b>personal data</b> for law enforcement purposes	<p>The Data Protection Act 2018, Part 3, Chapter 2, Section 35(2) outlines the legal bases for sharing personal data for law enforcement purposes. The processing is based on law and (select one):</p> <p><input type="checkbox"/> 35(2)(a) The data subject has given consent.</p> <p>_____ or _____</p>
	<p><input checked="" type="checkbox"/> 35(2)(b) The processing is necessary for the performance of a task carried out for that purpose by a competent authority.</p>

<b>Sensitive processing / processing special categories of personal data</b> for law enforcement purposes	<p><i>These legal bases also require an Appropriate Policy Document, each organisation should meet this requirement prior to sharing.]</i></p> <p>The Data Protection Act 2018, Part 3, Chapter 2, Section 35(3) outlines the legal bases for sharing sensitive / special categories of data for law enforcement purposes.</p> <p>The legal basis is (select one):</p> <p><input type="checkbox"/> 35(4) The data subject has given consent</p> <p style="text-align: center;">_____ or _____</p>
	<p><input checked="" type="checkbox"/> 35(5) The processing is strictly necessary for the law enforcement purpose, and</p> <p>Meets a relevant condition in Schedule 8. The relevant condition is:</p> <p><i>Statutory etc purposes</i></p> <p>1(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and (b) is necessary for reasons of substantial public interest.</p>

## 5 Personal information to be shared

- 5.1 Only the **minimum necessary** personal information consistent with the purposes set out in this document can be shared. Anonymised and pseudonymised information should be used where possible.
- 5.2 Information provided by partner organisations will not generally be released to any third party without prior consultation with the originating partner organisation.
- 5.3 An information reference table at Appendix B provides details of the information exchanges associated with this ISP, including the typical categories of information shared, the organisations involved and the parts of the organisation typically involved. As controllers in their own right, partner organisations are responsible for ensuring the appropriate staff have access to personal information that is adequate, relevant and limited to what is necessary for the intended purpose.
- 5.4 The following table sets out the personal information commonly shared to identify data subjects and ensure partner organisations are referring to the same data subject:

Personal identifiers	Select all that apply
Name (including aliases)	<input checked="" type="checkbox"/>
Date of birth	<input checked="" type="checkbox"/>
Address	<input checked="" type="checkbox"/>
Postcode	<input checked="" type="checkbox"/>
Gender	<input checked="" type="checkbox"/>
Other reference number (NHS number, Cardiff Council system/service number )	<input type="checkbox"/>

## 6 Data Subjects' Rights

- 6.1 Data protection legislation provides various individual rights for data subjects. Advice on how these rights should be met should be sought from each organisation's Information Governance representative, Data Protection Officer or equivalent. Specific guidance on these rights is available on the Information Commissioner's website; [www.ico.org.uk](http://www.ico.org.uk)
- 6.2 The following paragraphs refer to key rights associated with sharing personal information.
- 6.3 Unless doing so would risk harm to them or others, or hinder any investigation or legal proceedings, data subjects should be informed how and why their personal information will be processed and who it is shared with (the Right to be Informed). Ideally, this information – often provided in what is commonly referred to as a privacy notice - will be provided at the first point of contact. It can be part of a registration / consent form or a standalone document.
- 6.4 A layered approach is often appropriate. This could involve a high level organisational statement supplemented by specific service level information; for example a website or leaflet and verbal information provided by a practitioner.
- 6.5 Information should be clear and particular care should be taken when relying on consent as the legal basis for sharing information, or where working with children, as there are additional requirements to consider. Further information on the 'Right to be Informed' is available on the Information Commissioner's website; [www.ico.org](http://www.ico.org)
- 6.6 For the purposes of this ISP, partner organisations should set out below how they meet the requirements of the Right to be Informed. Ideally, a consistent message will be provided, and it may be helpful to agree a standard service level privacy notice.

Name of Organisation	Method of Informing (select any that apply)	Name of document / website	Comments
Cardiff Community Safety Partnership  (This includes the following partners: <ul style="list-style-type: none"> <li>• Cardiff Council;</li> <li>• South Wales Police &amp; Crime Commissioner's Office;</li> <li>• South Wales Police;</li> <li>• Cardiff &amp; Vale University Health Board</li> <li>• South Wales Fires &amp; Rescue Service</li> <li>• Third Sector Council</li> <li>• Safer Wales</li> </ul>	Website <input checked="" type="checkbox"/> Leaflet <input type="checkbox"/> Form <input type="checkbox"/> Verbal <input type="checkbox"/> Other (specify in comments) <input checked="" type="checkbox"/>	Privacy statement	An overall privacy statement drafted and put website <a href="#">Community Safety Partnership - Cardiff Partnership : Cardiff Partnership</a>
Cardiff and Vale University Health Board	Website <input checked="" type="checkbox"/> Leaflet <input type="checkbox"/>	<a href="https://cavuhb.nhs.wales/use-of-site/privacy-policy">https://cavuhb.nhs.wales/use-of-site/privacy-policy</a>	

	Form <input type="checkbox"/> Verbal <input type="checkbox"/> Other ( <i>specify in comments</i> ) <input type="checkbox"/>		
His Majesty's Prison & Probation Service	Website <input type="checkbox"/> Leaflet <input checked="" type="checkbox"/> Form <input type="checkbox"/> Verbal <input type="checkbox"/> Other ( <i>specify in comments</i> ) <input type="checkbox"/>	<a href="https://assets.publishing.service.gov.uk/media/60b7d1a0e90e07438a92dd4b/NPS-Privacy-Notice.pdf">https://assets.publishing.service.gov.uk/media/60b7d1a0e90e07438a92dd4b/NPS-Privacy-Notice.pdf</a>	
Shared Regulatory Services	Website <input checked="" type="checkbox"/> Leaflet <input type="checkbox"/> Form <input type="checkbox"/> Verbal <input type="checkbox"/> Other ( <i>specify in comments</i> ) <input type="checkbox"/>	<a href="https://www.srs.wales/en/Privacy-and-Cookies.aspx">https://www.srs.wales/en/Privacy-and-Cookies.aspx</a>	
British Transport Police	Website <input checked="" type="checkbox"/> Leaflet <input type="checkbox"/> Form <input type="checkbox"/> Verbal <input type="checkbox"/> Other ( <i>specify in comments</i> ) <input type="checkbox"/>	<a href="https://www.btp.police.uk/hyg/btp/privacy-notice/">https://www.btp.police.uk/hyg/btp/privacy-notice/</a>	
South Wales Violence Prevention Unit	Website <input checked="" type="checkbox"/> Leaflet <input type="checkbox"/> Form <input type="checkbox"/> Verbal <input type="checkbox"/> Other ( <i>specify in comments</i> ) <input type="checkbox"/>		
Safer Wales	Website <input checked="" type="checkbox"/> Leaflet <input type="checkbox"/> Form <input type="checkbox"/> Verbal <input type="checkbox"/>		

	Other ( <i>specify in comments</i> ) <input type="checkbox"/>		
For Cardiff	Website <input checked="" type="checkbox"/> Leaflet <input type="checkbox"/> Form <input type="checkbox"/> Verbal <input type="checkbox"/> Other ( <i>specify in comments</i> ) <input type="checkbox"/>	<a href="https://www.forcardiff.com/for-cardiff-contact-us/for-cardiff-privacy-policy/">https://www.forcardiff.com/for-cardiff-contact-us/for-cardiff-privacy-policy/</a>	
Victim Support	Website <input checked="" type="checkbox"/> Leaflet <input type="checkbox"/> Form <input type="checkbox"/> Verbal <input type="checkbox"/> Other ( <i>specify in comments</i> ) <input type="checkbox"/>	<a href="https://www.victimsupport.org.uk/privacy-policy-0/">https://www.victimsupport.org.uk/privacy-policy-0/</a>	
Action For Children	Website <input checked="" type="checkbox"/> Leaflet <input type="checkbox"/> Form <input type="checkbox"/> Verbal <input type="checkbox"/> Other ( <i>specify in comments</i> ) <input type="checkbox"/>	<a href="https://www.actionforchildren.org.uk/privacy-policy/">https://www.actionforchildren.org.uk/privacy-policy/</a>	
Crimestoppers	Website <input checked="" type="checkbox"/> Leaflet <input type="checkbox"/> Form <input type="checkbox"/> Verbal <input type="checkbox"/> Other ( <i>specify in comments</i> ) <input type="checkbox"/>	<a href="https://crimestoppers-uk.org/privacy-policy">https://crimestoppers-uk.org/privacy-policy</a>	
Vinci	Website <input checked="" type="checkbox"/> Leaflet <input type="checkbox"/> Form <input type="checkbox"/> Verbal <input type="checkbox"/> Other ( <i>specify in comments</i> ) <input type="checkbox"/>		

- 
- 6.8 All participating organisations will have in place policies and procedures to uphold the confidentiality, integrity and availability of personal information with specific reference to the retention, storage and disposal of records.
  - 6.9 Requests for the information referenced in this ISP will be dealt with in accordance with each partner organisation's relevant policies and procedures.
  - 6.10 Each partner organisation will put in place a formal procedure by which data subjects, partner organisations and practitioners can direct any complaints regarding the information sharing documented in this ISP.
  - 6.11 There is an expectation that partners to this ISP will work together to keep all partners informed of any complaints or requests for information received from data subjects or third parties. The partners will also keep each other informed of any problems associated with the information sharing practices documented in this ISP and there is an expectation that they will collaborate to develop and improve these practices.

## **7 Information security**

- 7.1 Each partner organisation must have an appropriate and adequate security framework.
- 7.2 Practitioners carrying out the functions outlined in this ISP should make themselves aware of, and adhere to, their organisation's information security policies and procedures.
- 7.3 A detailed list of agreed methods for the safe and secure transfer of personal information is documented within Appendix B.
- 7.4 All partners must ensure adequate and appropriate training on the subjects of data protection and confidentiality is provided to all staff with access to personal data.

## **8 Review, Breaches and Termination of this Agreement**

- 8.1 This ISP will be reviewed two years from signing this document or sooner if appropriate. There is guidance available on the WASPI website about the process for reviewing an ISP.
- 8.2 Breaches of this agreement should be reported to the Owners / Contact Points in Section 2, which may result in the information sharing set out in this agreement ceasing.
- 8.3 Partners to this agreement will determine the responsibilities following termination of this agreement, including the deletion of shared data or its return to the organisation that supplied it originally.

## 9 Appendix A – Glossary of Terms

Term	Definition
<b>Appropriate Policy Document</b>	<p>The Data Protection Act 2018 outlines the requirement for an Appropriate Policy Document to be in place when processing special category and criminal offence data under certain specified conditions.</p> <p>Detail on Appropriate Policy Documents can be found in Schedule 1, Part 4 of the DPA 18 and Section 42 of the DPA 18 for competent authorities.</p>
<b>Data Protection Act 2018</b>	<p>The UK’s third generation of data protection law replaces the Data Protection Act 1998. The 2018 Act accepts the standards and obligations set by UK GDPR and, where UK GDPR allows, makes specific provisions relevant to the UK.</p> <p>The 2018 Act also transposes EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law.</p> <p>It is important the UK GDPR and the DPA 2018 are read side by side.</p>
<b>Data Protection Officer</b>	<p>Certain categories of organisation, including any public body or authority (except courts in their judicial capacity) are required to designate a suitably qualified Data Protection Officer (DPO). The tasks of the DPO are set out in Article 39 of UK GDPR.</p>
<b>Data subject</b>	<p>A ‘data subject’ is an identified or identifiable natural person. Organisations may refer to data subjects as service users, patients, clients, citizens, etc but for consistency, WASPI framework documentation refers to data subjects.</p>
<b>UK GDPR</b>	<p>The UK General Data Protection Regulation (UK GDPR) lays down laws relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.</p>
<b>Law Enforcement Purposes</b>	<p>The 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 (DPA 2018 Part 3, Chapter 1, Section 31).</p>
<b>Personal data</b>	<p>‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</p>

<b>Personal data about criminal convictions, offences or related security measures</b>	This includes personal data which relates to the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing. (DPA 2018 Section 11(2))
<b>Personal identifiers</b>	A set of basic personal details that allow partner organisations to identify a data subject.
<b>Personal information</b>	Includes information falling within the definition of 'personal data' and information about deceased individuals. Data protection legislation does not apply to information about deceased individuals but such information needs to be treated confidentially and WASPI should be applied to this information.
<b>Practitioner</b>	An inclusive term that refers to those involved in the care, education, welfare of data subjects; ie those who provide a public service.
<b>Processing personal data</b>	'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.' (UK GDPR Art 4(2))
<b>Special categories of data / sensitive processing</b>	Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. (UK GDPR Art 9(1))
<b>[Insert further terms as appropriate]</b>	

## 10 Appendix B – Information Reference Table for Cardiff Community Safety Partnership

This table sets out the why, what, when and how of information sharing in detail. Guidance on completing this section can be found on the website

	Description	Context/Incident	Analysis	Collaboration	Evaluation
1	<p><b>Information exchange</b></p> <p><i>General description of the process or stage to which the information sharing relates.</i></p>	Information/data regarding Community Safety issues to the Cardiff Council and South Wales Police Community Safety Teams by any organisation/agency.	Assessment/analysis undertaken by Community Safety Team and brought to Partnership priority meeting area or Subgroup for partnership showcasing/discussion and interpretation.	Cardiff Council Community Safety Team can share further relevant information with agencies involved in the Partnership meetings work, to further inform or progress an identified issue.	<p>Relevant Agency/ Subgroups collectively evaluate interventive work.</p> <p>Determine the need for onward referral to a single agency for further intervention, a return to the collaboration phase, or acknowledge the resolution of the issue.</p>
2	<p><b>What information will be shared?</b></p> <p><i>Describe the information to be shared – you do not need to go to ‘field level’ detail.</i></p> <p><b><u>Please note: Only the minimum and relevant personal information is to be shared and strictly on a case by case basis.</u></b></p>	<p>Agreed data sets that would contribute towards understanding the priority areas of the community safety partnership: Violence Prevention Group, Street Based Lifestyles, Problem Solving Group and supporting subgroups. This may include personal identifiers such as; demographic data, health and wellbeing, offending history, risk assessment or safeguarding issues, family history or personal profile, medical health history/substance misuse information.</p>	<p>Presentation documents such as Dashboards, reports, data sets might be used to display findings for the meetings which may include high level representations of, some personal identifiers, demographic data, health and wellbeing, offending history, risk assessment or safeguarding issues, family history or personal profile, medical health history/substance misuse information.</p>	<p>Agreed information (data sets, reports, dashboards) that would contribute to informing partnership understanding. This may include high level personal identifiers, demographic data, health and wellbeing, offending history, risk assessment or safeguarding issues, family history or personal profile, medical health history/substance misuse information.</p>	<p>Service level performance information for the purposes of evaluating interventions collectively. The level of information shared would be tailored to the specific circumstances to understand the context and best practice.</p>

	Description	Context/Incident		Analysis		Collaboration		Evaluation	
		Who by	Who to	Who by	Who to	Who by	Who to	Who by	Who to
3	<p><b>Partner Organisation(s)</b></p> <p><i>Details of provider and recipient organisation(s)</i></p> <p><i>Ensure the organisations listed reflect section 2 of the ISP i.e. are all organisations listed in section 2</i></p>	All partners listed in Table 2	<p>Cardiff Council Community Safety Team</p> <p>and South Wales Police Community Safety</p>	<p>Cardiff Council Community Safety Team</p> <p>and South Wales Police Community Safety</p>	All partners listed in Table 2	All partners listed in Table 2	All partners listed in Table 2	All partners listed in Table 2	All partners listed in Table 2
4	<p><b>How is information shared and what methods are used to keep the information secure?</b></p> <p><i>Provide, in detail the specific agreed secure methods for sharing personal information</i></p>	<p>Secure email, either using TLS1.2 or encrypted email.</p> <p>Portals/Dashboards.</p> <p>Multi-Agency meetings.</p> <p>South Wales Police data is provided via a police encrypted laptop and emailed to a Council encrypted laptop.</p>	<p>Secure email, either using TLS1.2 or encrypted email.</p> <p>Portals/Dashboards.</p> <p>Multi-Agency meetings.</p> <p>South Wales Police is provided via a police encrypted laptop and emailed to a Council encrypted laptop.</p>	<p>Secure email, either using TLS1.2 or encrypted email.</p> <p>Portals/Dashboards.</p> <p>Multi-Agency meetings.</p> <p>South Wales Police is provided via a police encrypted laptop and emailed to a Council encrypted laptop.</p>	<p>Secure email, either using TLS1.2 or encrypted email.</p> <p>Portals/Dashboards.</p> <p>Face to face meeting or secure online meeting (Microsoft Teams)</p>	<p>Secure email, either using TLS1.2 or encrypted email.</p> <p>Portals/Dashboards.</p> <p>Face to face meeting or secure online meeting (Microsoft Teams)</p>	<p>Secure email, either using TLS1.2 or encrypted email.</p> <p>Portals/Dashboards.</p> <p>Face to face meeting or secure online meeting (Microsoft Teams)</p>	<p>Secure email, either using TLS1.2 or encrypted email.</p> <p>Portals/Dashboards.</p> <p>Face to face meeting or secure online meeting (Microsoft Teams)</p>	<p>Secure email, either using TLS1.2 or encrypted email.</p> <p>Portals/Dashboards.</p> <p>Face to face meeting or secure online meeting (Microsoft Teams)</p>

	Description	Context/Incident	Analysis	Collaboration	Evaluation
5	<b>Reliance on consent</b> <i>Check the box if any exchange relies on consent and explain how and when consent is obtained. Ensure section 4 of the ISP reflects this legal basis</i>	<input type="checkbox"/> Exchange relies on consent. <input checked="" type="checkbox"/> Exchange does not rely on consent.	<input type="checkbox"/> Exchange relies on consent. <input checked="" type="checkbox"/> Exchange does not rely on consent.	<input type="checkbox"/> Exchange relies on consent. <input checked="" type="checkbox"/> Exchange does not rely on consent.	<input type="checkbox"/> Exchange relies on consent. <input checked="" type="checkbox"/> Exchange does not rely on consent.
6	<b>Notes for Practitioners</b>				

## 11 Appendix D – Data Owner Reference Table

Data Set	Owner / Point of contact	Departments / Divisions / Teams	Organisation
ASB and Crime Data	PCSO/NICHE Database	Cardiff Neighbourhood Policing Team	British Transport Police
Harm Reduction Database	Head of Substance Misuse Strategy, Partnerships and Commissioning	Substance Misuse & Harm Reduction	Cardiff and Vale University Health Board
Ambulance Callout Data	Patient Experience & Community Involvement Coordinator	Community Involvement	Cardiff and Vale University Health Board
A&E Assault Related Attendances Data	Information Officer	Information Department	Cardiff and Vale University Health Board
Community Safety Reports & Compiled Data Sets	Community Safety Project Manager/Senior Partnership Analyst	Community Safety	Cardiff Council

Support Living Accommodation Data	Antisocial Behaviour Manager/ Managed Accommodation Service Manager	Housing & Communities	Cardiff Council
Homeless Data & Rough Sleeper Update	Improvement Project Manager	Adults, Housing & Communities	Cardiff Council
Safeguarding Observations/Trends	Senior Policy Officer	SAFE partnership	Cardiff Council
Street Cleansing Outcomes/iAuditor Data	Senior Collections & Cleansing Officer	Recycling & Neighbourhood Services	Cardiff Council
Referral Data	OM Youth Offending Services	Youth Offending Services	Cardiff Council
Referral Data	Manager, Youth Services	Youth Justice Service	Cardiff Council
Exclusions, Truancy, Incidents	Project Manager	Education Welfare	Cardiff Council
Child Friendly Cardiff Pupil Survey	Child Friendly Co-Ordinator	Child Friendly Cardiff	Cardiff Council
Ask Cardiff - Annual Public Survey	Principal Research & Consultation Officer	Research Team	Cardiff Council
Footfall, PSS, Park Activity Data	Parks Community Safety Manager	Parks Team	Cardiff Council
Geographic Information Resources (CCTV, Area Boundaries, etc.)	Various (data is freely available but subject to PSMA licence terms)	Various/Corporate GIS Team	Cardiff Council
Drug Litter Data	Senior Business Analyst	Communities & Customer Services	Cardiff Council
Children's Social Care Data		Children's Services	Cardiff Council
Family Help Assessments	Family Gateway & Early Help Manager	Wellbeing Protection & Support	Cardiff Council
Exploitation Data	Operational Manager Shared Regulatory Services	(CC) Shared Regulatory Services/Commercial Services and Trading Standards/ Wales Illegal Money Lending Unit (WILMLU)	Cardiff Council
Proactive Drug Litter Collection Data	Project Manager	Facilities	Cardiff Council
Crime, ASB, and Reported Concerns	Fearless Outreach Worker	Local Team	Crimestoppers
Cleansing Data	Evening and Nighttime Economy Manager & Project Manager	Project Management	For Cardiff

Trend and Profile Data	Governor	Prison Services	His Majesty's Prison and Probation Services Cardiff
Offender Profile Data	Deputy Head of Probation Service/Head of Probation Delivery Unit	Probation Delivery	His Majesty's Prison and Probation Services Cardiff
Public Litter Reporting Reports and Trends	ICT and Data Manager Director of Project Development	Keep Wales Tidy Safer Wales	Keep Wales Tidy Safer Wales
ASB and Fire Reports	Fire Crime Practitioner, Fire Crime Unit	Operations Management	South Wales Fire and Rescue Services
ASB and Crime Data	PCSO	Cardiff Neighbourhood Policing Team	South Wales Police
ASB and Crime Data Reports and Trends	Cardiff and Vale Command Unit/ Superintendent for Partnership Victim Support Officer	Community Safety Local Team	South Wales Police Victim Support
Referral Data & Safe Mapping Data	Service Coordinator	Sidestep Cardiff	Violence Prevention Unit