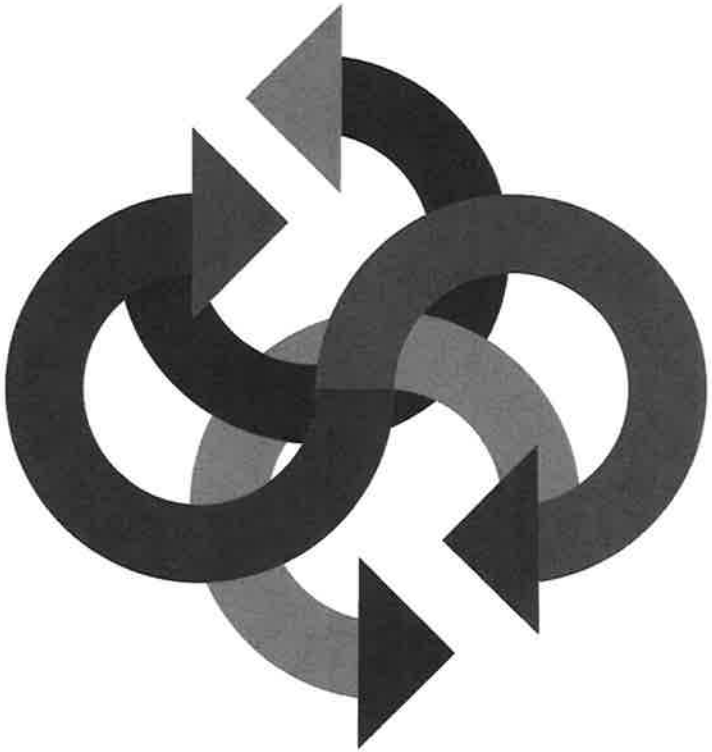

Wales Accord on the
Sharing of Personal Information

Information Sharing Protocol for

Powys Community Safety Partnership

Version	Final V1
Date Assured	29 October 2018
Quality Assurance Group	Mid and West Wales

Contents

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

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 for Powys Community Safety Partnership in Powys

1.4 Personal information is shared for the purpose of tackling crime, disorder and substance misuse issues within Powys. To enable the delivery of multi-agency Serious Organised Crime groups, Neighbourhood Management Groups, Domestic Homicide Reviews and Channel Panels:-

Serious Organised Crime group – Tactical, multi-agency group, chaired by police to enable partnership working to tackle serious organised crime under specific Police Operations.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf

Neighbourhood Management groups – Multi-agency group, convened to tackle a specific community issue which is impacting upon quality of life.
http://pstatic.powys.gov.uk/fileadmin/Docs/Democracy/2nd_Map_-_NEIGHBOURHOOD1_MANAGEMENT_TOOLKIT.pdf

Domestic Homicide Reviews – statutory duty for a Community Safety Partnership to conduct Domestic Homicide Reviews – the review panel is a multi-agency panel.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/97881/DHR-guidance.pdf

Channel Panels – Channel Panels are part of the Home Office PREVENT strategy. Consent is required. There is a PREVENT duty on all statutory organisations.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf

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
Powys Teaching Health Board	Executive Lead for Safeguarding	Safeguarding Mental Health
National Probation Service	Head of Dyfed Powys Local Delivery Unit	Powys Delivery Unit
Dyfed-Powys Police	Partnerships Chief Inspector	Neighbourhood Policing Roads Policing

		Response Offender Management
Mid & West Wales Fire & Rescue Service	Head of Community Safety	Community Safety Arson Reduction Team Road Safety
Powys Youth Justice Service	Youth Offending Team Manager	Powys Youth Justice Service
Powys Association of Voluntary Organisations	Head of Third Sector Development	All teams
Powys County Council	Head of Service – Regulatory and Planning	Trading Standards, Housing, Adult Safeguarding, Child Safeguarding, Licencing, Environmental Health Education Road Safety

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 owner / 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

4.1 The sharing arrangements described in this ISP take into account the relevant data

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

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

4.5 In order for sharing to be lawful:

- At least one legal basis in each of the two tables below needs to be met (this is based on the assumption that services supported by ISPs will be processing special categories of data / undertaking sensitive processing).
- Organisations need to be specific and should not normally select more than one legal basis per table.
- Where more than one legal basis is selected, an explanation should be provided in the Pre Quality Assurance Checklist.

4.6 The legal bases have been streamlined to those likely to be most relevant to public service providers. Other legal bases exist and may be added to the table if required. Clear notes should be added to explain how any additional legal basis is relevant.

4.7 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 and 9 of 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.

4.8 Consent to process personal data should not be confused with consent to treat patients. The two are separate and should not be confused or merged.

Article 6 Legal Bases for Sharing Personal Data

Legal basis	Check box / Notes
General processing	
Consent – Art 6(1)(a)	☒ *Consent is used specifically for Channel Panels – this is pre-criminal and voluntary.*
Necessary for compliance with a legal obligation – Art 6(1)(c)	☒ • *The Crime and Disorder Act 1998 Section 115 states "relevant authorities have the power… to share information if it is necessary for the purposes of any provision under the Crime and Disorder Act. This would include where it is necessary for the formulation and implementation of the local Crime and Disorder Reduction Strategy".* • *Article 8 of the Human Rights Act is the article of particular relevance to information sharing for community safety. It states that everyone has the right to respect for their private and family life, home and correspondence, and that no public authority will interfere with this right unless it is necessary by law. This qualification will usually enable personal information to be shared on the following grounds: national security, public safety, economic wellbeing of the country, to prevent crime or disorder, to protect health or morals, and to protect the rights or freedoms of others.*
Is there processing for law enforcement purposes?	☒ *The Data Protection Act 2008, Part 3;* *Section 35(2)(a) – the data subject has given consent* ***[Channel Panels only]*** *Section 35(2)(b) – the processing is necessary for the performance of a task carried out by a competent authority* ***[All other sharing described by this ISP]***

Article 9 Legal Bases for Sharing Special Categories of Personal Data

Legal basis	Checkbox / Notes
General processing	
Explicit Consent – Art 9(2)(a)	☒ *Consent is used specifically for Channel Panels – this is pre-criminal and voluntary.*
Necessary for reasons of substantial public interest - Art 9(2)(g)	☒
Is there processing for law enforcement purposes?	☒ *The Data Protection Act 2018, Part 3* *To the extent data is sensitive (see section 35(8):* *Section 35(4)(a) & (b) – the data subject has given consent and an appropriate policy document is in place* ***[Channel Panels only]*** *Section 35(5)(a),(b) & (c) – the processing is strictly necessary for the law enforcement purpose, meets at least one of the conditions*

	in Schedule 8 and an appropriate policy document is in place ***[All other sharing described by this ISP]*** *The relevant condition(s) in Schedule 8 are* 1. *Statutory etc purposes;* 2. *Administration of justice* 3. *Protecting individuals' vital interests* 4. *Safeguarding of children and of individuals at risk*

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 necessary.

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)	☒
Date of birth	☒
Address	☒
Postcode	☒
Other reference number (eg NHS number, National Insurance number, any system/service number)	☒

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

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

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 *(eg website address, leaflet/form name)*	Comments
Powys teaching Health Board	Website ☒ Leaflet ☒ Form ☐ Verbal ☒ Other ☐ (specify in comments)	http://www.powysthb.wales.nhs.uk/page/80765 http://www.powysthb.wales.nhs.uk/sitesplus/documents/1145/your%20rights.pdf	
National Probation Service	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other ☐ (specify in comments)	https://www.gov.uk/government/organisations/ministry-of-justice/about/personal-information-charter	
Dyfed-Powys Police	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments)	https://www.dyfed-powys.police.uk/en/about-us/how-we-will-use-your-information/fair-processing-statement/ Further information on website - https://www.dyfed-powys.police.uk/en/about-us/how-we-will-use-your-information/	
Mid & West Wales Fire Service	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other ☐ (specify in comments)	http://www.mawwfire.gov.uk/english/pages/privacy.aspx	
Powys Youth Justice Service	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other ☐ (specify in comments)	http://www.powys.gov.uk/en/information-mangement/data-protection-and-privacy/	
PAVO	Website ☒ Leaflet ☐ Form ☐	https://www.pavo.org.uk/about-pavo/privacy-policy.html	

	Verbal ☐ Other ☐ (specify in comments)	Further information on website - https://www.pavo.org.uk/about-pavo/legal-information.html	
Powys County Council	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other ☐ (specify in comments)	http://www.powys.gov.uk/en/information-mangement/data-protection-and-privacy/	

6.7 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.

6.8 Requests for the information referenced in this ISP will be dealt with in accordance with each partner organisation's relevant policies and procedures.

6.9 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 practices documented in this ISP.

6.10 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 collaborative 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 of this ISP

8.1 This ISP will be reviewed two years from signing this document or sooner if appropriate.

9 *Appendix A – Glossary of Terms*

Term	Definition
Data Protection Act 2018	The UK's third generation of data protection law replaces the previous Data Protection Act 1998. The 2018 Act accepts the standards and obligations set by GDPR and, where GDPR allows, makes specific provisions relevant to the UK. The 2018 Act also transposes EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law. It is important the GDPR and the DPA 2018 are read side by side.
Data Protection Officer	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 GDPR.
Data subject	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.
GDPR	The General Data Protection Regulation (GDPR) lays down rules 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.
Personal data	'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.
Personal identifiers	A set of basic personal details that allow partner organisations to identify a data subject.
Personal information	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.
Practitioner	An inclusive term that refers to those involved in the care, education, welfare of data subjects; ie those who provide a public service.

Processing personal data	'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.' (GDPR Art 4(2))
Special categories of data / sensitive data	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. (GDPR Art 9(1)) Personal information relating to criminal convictions and offences or related security measures (GDPR Art 10).

10 Appendix B – Information Reference Table for Powys 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 here

	Description	Referral		Allocation		Intervention		Onward Referral	
1	**Information exchange** *General description of the process or stage to which the information relates*	**Referrals** - Initial referral into the Powys Community Safety Partnership in relation to Domestic Homicide Reviews, Channel Cases, Neighbourhood Management, Serious Organised Crime		**Allocation** - Filter referrals by the Powys Community Safety Partnership Co-ordinator for assessment or signpost to other Agencies / Sub Groups if appropriate.		**Intervention** - Agency / Sub Group to assess in detail to develop an action plan to deliver response and report on progress.		Onward referral to single agency to facilitate further intervention if necessary.	
2	**What information will be shared?** *Describe the information to be shared – you do not need to go to 'field level' detail.* ***Please note: Only the minimum and relevant personal information is to be shared and strictly on a case by case basis.***	Personal Identifiable Information (Full Name, Address, DOB) Plus reason for referral e.g. Domestic Homicide Review, Channel Case, Neighbourhood Management, Serious Organised Crime		Personal Identifiable Information (Full Name, Address, DOB) Plus reason for referral e.g. Domestic Homicide Review, Channel Case, Neighbourhood Management, Serious Organised Crime		Personal Identifiable Information (Full Name, Address, DOB) Concerns relating to the person / family / in relation to Domestic Homicide Review, Channel Case, Neighbourhood Management, Serious Organised Crime		The minimum amount of information to provide an effective service. Personal Identifiable Information (Full Name, Address, DOB)	
3	**Partner Organisation(s)**	**Who by**	**Who to**	**Who by**	**Who to**	**Who by**	**Who to**	**Who by**	**Who to**

Details of provider and recipient organisation(s) *Ensure the organisations listed reflect section 2 of the ISP i.e. are all organisations listed in section 2*	1. Powys Teaching Health Board 2. National Probation Service 3. Dyfed-Powys Police 4. Mid & West Wales Fire & Rescue Service 5. Powys Youth Justice Service 6. Powys Association of Voluntary Organisations 7. Powys County Council	1. Powys Community Safety Partnership Co-ordinator	1. Powys Community Safety Partnership Co-ordinator	1. Powys Teaching Health Board 2. National Probation Service 3. Dyfed-Powys Police 4. Mid & West Wales Fire & Rescue Service 5. Powys Youth Justice Service 6. Powys Association of Voluntary Organisations 7. Powys County Council	1. Powys Teaching Health Board 2. National Probation Service 3. Dyfed-Powys Police 4. Mid & West Wales Fire & Rescue Service 5. Powys Youth Justice Service 6. Powys Association of Voluntary Organisations 7. Powys County Council	1. Powys teaching Health Board Safeguarding 2. National Probation Service Powys LDU 3. Dyfed-Powys Police Powys Division IOM WISDOM 4. Mid & West Wales Fire & Rescue Service Community Safety Arson Reduction Unit Road Safety 5. Powys Youth Justice Service 6. Powys Association of Voluntary Organisations 7. Powys County Council (all depts.)	1. Powys Teaching Health Board 2. National Probation Service 3. Dyfed-Powys Police 4. Mid & West Wales Fire & Rescue Service 5. Powys Youth Justice Service 6. Powys Association of Voluntary Organisations 7. Powys County Council	1. Powys teaching Health Board Safeguarding 2. National Probation Service Powys LDU 3. Dyfed-Powys Police Powys Division IOM WISDOM 4. Mid & West Wales Fire & Rescue Service Community Safety Arson Reduction Unit Road Safety 5. Powys Youth Justice Service 6. Powys Association of Voluntary Organisations 7. Powys County Council (all depts.)

	Description	Referral	Allocation	Intervention	Onward Referral
4	**What safeguards are in place to protect the information referred to in row 2, above?** *Provide, in detail the specific agreed secure methods for sharing personal information*	Telephone E-mail – secure – GCSX; CJSM Password Protected documents via e-mail Direct feed from IT systems	Telephone Verbal – at relevant meeting E-mail - secure e-mail – GCSX; CJSM Password Protected documents via e-mail	Telephone Verbal – at relevant meeting E-mail - secure e-mail – GCSX; CJSM Password Protected documents via e-mail	Telephone Verbal – at relevant meeting E-mail - secure e-mail – GCSX; CJSM Password Protected documents via e-mail
5	**Reliance on consent** *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*	☒ Exchange relies on consent ☒ Exchange does not rely on consent Consent is required in relation to **Channel Panels only**. The Consent is obtained by Police when meeting the individual prior to referral to the Channel Panel.	☒ Exchange relies on consent ☒ Exchange does not rely on consent Consent is required in relation to **Channel Panels only**. The Consent is obtained by Police when meeting the individual prior to referral to the Channel Panel.	☒ Exchange relies on consent ☒ Exchange does not rely on consent Consent is required in relation to **Channel Panels only**. The Consent is obtained by Police when meeting the individual prior to referral to the Channel Panel.	☒ Exchange relies on consent ☒ Exchange does not rely on consent Consent is required in relation to **Channel Panels only**. The Consent is obtained by Police when meeting the individual prior to referral to the Channel Panel.
6	**Notes for Practitioners**				