



Response Date:08/05/2024

2024/443 - Sharing Agreement

In response to your recent request for information regarding;

1. The MARAC Information Sharing Agreement for North Wales and details of all the parties involved.

Please find attached 6 x Information Sharing Agreements, one for each local authority area.

2. The Operating Protocol or Guidance for the MARAC in North Wales.

Please find attached the North Wales MARAC Operating Protocol, please note the document is under review.

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST
UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 07/05/2024



NORTH WALES MARAC OPERATING PROTOCOL

North Wales MARAC Operating Protocol

Table of Contents

1) Introduction.....	2
2) Partner Agencies.....	4
a) Role of the MARAC representative	4
b) New MARAC Representatives/agencies attending MARAC	5
c) Induction and Training for a MARAC representative	6
3) Governance and Performance Management.....	7
4) Process of the MARAC	8
a) Criteria for MARAC	8
b) Referral	8
c) MARAC agenda.....	8
d) Actions before the MARAC.....	9
e) Weekly MARAC meeting.....	9
f) Monthly MARAC meeting.....	10
g) Role of the Chair.....	11
h) Information sharing –	11
i) Risk action Planning	11
j) Transfers.....	11
5) Equality	12
6) Evaluation	12
7) Withdrawal.....	12
8) Signatories.....	12

1) Introduction

The purpose of this MARAC Operating Protocol (MOP) is to establish regional accountability and responsibility for the weekly and monthly MARAC within the North Wales region. Additionally this protocol outlines the various processes and procedures of the MARAC.

The protocol is designed to enhance existing arrangements for safeguarding children and adults, as well as those for public protection, rather than replace them and has a particular focus on victim's and children's safety.

North Wales MARACs will work with individuals deemed at high risk of harm or homicide who meet the definition of Domestic Abuse as defined by Welsh Governments' Violence against Women, Domestic Abuse and Sexual Violence (Wales) Act 2015.

Welsh Government has adopted the definition utilised by the Council of Europe Convention and the United Nations.

The UN Declaration defines violence against women as:

' All acts of gender-based violence that result in, or are likely to result in, physical, sexual, psychological, or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life'

This encompasses, but is not limited to:

(a) Physical, sexual and psychological violence occurring in the family, including battering, sexual abuse of female children in the household, dowry-related violence, marital rape, female genital mutilation and other traditional practices harmful to women, non-spousal violence and violence related to exploitation;

(b) Physical, sexual and psychological violence occurring within the general community, including rape, sexual abuse, sexual harassment and intimidation at work, in educational institutions and elsewhere, trafficking in women and forced prostitution;

(c) Physical, sexual and psychological violence perpetrated or condoned by the State, wherever it occurs.

Whilst Welsh Government acknowledges and communicates the disproportionate experience of women and girls this does not negate violence and abuse directed towards men and boys or perpetrated by women. The VAWDASV Act recognises that anyone (women, men, children and young people) can experience and be affected by domestic abuse or sexual violence.

The aims of the MARAC are:

1. To provide a regular forum for inter-agency sharing of information in order to increase the safety, health and wellbeing of victims – adults and their children.
2. To determine whether the perpetrator poses a significant risk to any particular individual or the general community.
3. To identify any gaps in the risk assessments in relation to victim, children or perpetrator, that require referral onward
4. To construct and implement a risk management plan that provides professional support to all those at risk and that reduces the risk of harm
5. To reduce repeat victimisation
6. To improve agency accountability
7. To improve support for staff involved with high risk Domestic Abuse cases

2) Partner Agencies

The following agencies are signatories to the regional MOP, as well as the regional MARAC Information Sharing protocols (which conform to the Wales Accord on Personal Information Sharing (WASPI)). Those regularly attending MARAC include: (this is not an exhaustive list and additional agencies may be invited to attend on an ad hoc basis by the Chair)

- North Wales Police (NWP)
- Betsi Cadwaladr University Health Board (BCUHB) – Safeguarding
- Betsi Cadwaladr University Health Board (BCUHB) – Mental Health services
- Betsi Cadwaladr University Health Board (BCUHB) – Substance Misuse services
- Isle of Anglesey County Council (IOACC) – to include Housing, Education, Social Services, Community Safety Partnership
- Gwynedd Council (GC) to include Housing, Education, Social Services, Community Safety Partnership
- Conwy County Council (CCC) to include Housing, Education, Social Services, Community Safety Partnership
- Denbighshire County Council (DCC) to include Housing, Education, Social Services, Community Safety Partnership
- Flintshire County Council (FCC) to include Housing, Education, Social Services, Community Safety Partnership
- Wrexham County Borough Council (WCBC) to include Housing, Education, Social Service, Community Safety Partnership
- National Probation Service (NPS)
- DASU North Wales
- Gorwel
- Clwyd Alyn Housing Association (CAHA)
- Wales and West Housing Association (WWHA)

a) Role of the MARAC representative

Each partner agency will appoint a MARAC representative to attend the monthly MARAC meetings (some will also attend the weekly MARAC meetings – NWP, BCUHB, Local Authorities, NPS, DASU, Gorwel). It is good practice for the agencies to nominate the same MARAC representative on an ongoing basis, for consistency. If the appointed representative is not able to attend, the agency is responsible for sending a deputy and ensuring they are in receipt of all relevant information. If the agency is too small to have the capacity to send a deputy, they should contact the MARAC Coordinator sufficiently in advance to inform the Chair, as well as sending any pertinent information they have to the Coordinator for discussion at the meeting.

No one subject to the risk or their personal representatives, will be invited to attend the MARAC.

The MARAC representative must have the authority to commit appropriate resources to the multi-agency risk management plan. The expectation is that the nominated representative will attend the whole meeting in order to provide an organisational perspective on all cases discussed, irrespective of whether the case is already known/open to them or not.

The MARAC representative is expected to have read the agenda in advance and gathered all appropriate information their agency holds regarding those subject to the MARAC, in order to share this information with the meeting.

The MARAC representative is expected to share all pertinent information held by their agency regarding their involvement with the person at risk (and/or their immediate family), including any completed actions, in order to inform the ongoing plan. If they have had no involvement with the person, they are expected to use their specialist knowledge to suggest improvements to the risk management plan. Information shared at the meeting should be pertinent to the cases and if historical information is shared, this must be in relation to the current case.

If a representative/agency repeatedly fails to attend the MARAC without informing the Chair and sending pre-prepared research, the Chair will approach the Service Manager from the agency involved to discuss. If the matter is not resolved to their satisfaction or the agency continually fails to attend, the matter will be raised with the Regional MARAC Steering Group. Any further concerns will be escalated to the Vulnerability and Exploitation Board.

All present at the MARAC are responsible for the smooth running of the Conference. If anyone attending MARAC is unhappy with information being shared, or how that information is communicated to the wider group, they have a responsibility to challenge that. They should voice any concerns at the meeting and to the Chair in the first instance and then to the Regional MARAC Steering Group if they are not happy with how the situation has been resolved.

b) New MARAC Representatives/agencies attending MARAC

If a new representative is appointed, or if the agency is new to the MARAC process, the agency must contact the MARAC Coordinator and inform them of the name, role and contact details of the new representative. Where this is practicable, this should be done prior to the change in representation. The new representative must also be sighted on the confidentiality statement (copy below)



CONFIDENTIAL.doc

Following the above procedure will give the employing agency time to ensure that their representative is provided with the Safe Lives MARAC toolkit. The toolkit is an aid to understanding the purpose of MARACs and the role and responsibilities of the MARAC representative.



MARAC
Representatives too

If a new agency wishes to attend MARAC on a regular basis, they must contact the MARAC Coordinator, who will take the request to the Regional MARAC/ADAPT Steering Group for discussion.

c) Induction and Training for a MARAC representative

A new MARAC representative should be given the Safe Lives MARAC Toolkit by their agency and offered training where available. If no formal training is available, new MARAC representatives should be supported to go through the agenda, research cases and present relevant information in preparation for the meeting, by an experienced member of staff. It is the responsibility of the employing agency to only send adequately prepared and trained MARAC representatives.

3) Governance and Performance Management

The North Wales MARAC/ADAPT Steering Group oversee the running of the MARACs across the region. This includes the development of any policies, changes to processes and scrutiny of decisions. If the Regional Steering Group are unable to resolve any issues or challenges, the Chair of the Steering Group will escalate it to the North Wales Vulnerability and Exploitation Board for a decision.

The Regional MARAC/ADAPT Steering Group has a responsibility to review the MARAC processes and ensure practice is in line with 'Safelives' guidance, *10 principles of an effective MARAC* (www.safelives.org.uk).

The MARAC steering group has the following functions:

- To review MARAC processes against practice standards (Safelives)
- To offer challenge and recommendations to agencies to ensure victims of domestic abuse are safe and protected from harm
- To monitor volume of cases heard at MARAC, identify trends, themes and referral structures
- To quality assure the decisions and actions agreed at MARAC by way of case auditing
- Monitor MARAC representation, attendance and quality of engagement from partner agencies
- Review data in relation to outcomes
- To consider changes in policy and research
- To promote consistency of processes across the six MARACs.
- Implement learning and recommendations from Domestic Homicide Reviews (DHRs) as appropriate

The Regional VAWDASV Advisor will report on the work of the North Wales MARAC/ADAPT Steering Group on a quarterly basis.

4) Process of the MARAC

a) Criteria for MARAC

The **Domestic Abuse Stalking Harassment and Honour Based Violence Risk Identification Checklist (DASH RIC)** is the main assessment tool used to determine the level of risk a survivor, her/his children and any vulnerable adults in the household are experiencing. This is also contained within the CID 16/EOEL:06 (NWP documentation). The level of risk can be assessed by the number of 'yes' ticks on the form, the frequency/severity of the abuse, as well as professional judgement. (See **b) Referral**). The Safe Lives Severity Grid can also be used with the DASH RIC to give a framework to identify features of the abuse suffered and support any decisions based on professional judgement. If the officer/professional completing the DASH ticks 14 or more boxes, it is an automatic referral to MARAC.

If that threshold has not been met, it is possible to still refer to MARAC, if in your 'professional judgement' it meets the threshold of high risk. This judgement allows professionals to utilise their understanding of the context of the situation and client/service user, their professional knowledge and their training in order to identify concerns and take relevant action. When using your professional judgement for high risk domestic abuse cases, you need to be able to provide rationale for why the referral is high risk. This will enable MARAC partners to have a clear and detailed understanding as to why the DASH RIC referral is high risk. Any rationale given should be clearly written on the MARAC referral, so to enable an eligibility decision

A case will always be referred to MARAC if there has been an escalation in risk and frequency of incidents. 3 incidents in 6 months will generate an automatic referral to MARAC. Repeat cases will be heard at MARAC if there has been another incident within 12 months.

b) Referral

All MARAC referrals should go to the Central Referral Unit within North Wales Police.

External referrals are sent to NWP via e mail on the approved referral document to: publicprotectionreferralunit@nthwales.police.uk where they may be tasked to a Domestic Abuse officer for review and preparation.

c) MARAC agenda

Once a case has been identified for Weekly MARAC, it will be heard at the following weekly meeting for that area without exception.

The weekly agenda (including case list) will be sent by email to all agencies before the end of the working day on Thursday of the previous week. It should include details of the subject, perpetrator, children, and a summary of the incident.

MARAC administrators will circulate MARAC documentation to partners via email and will include the TEAMS link to the meeting:

The key agencies required to attend the weekly meeting include (but not limited to):

IDVA services

Domestic Abuse specialist services (if different to IDVA providers)

Children's Social Services

BCUHB – Safeguarding

BCUHB – Mental Health

National Probation Services

Adult Social Services

The circulation lists for the weekly and monthly MARACs are the same, but the expectation is that only core agencies attend the weekly virtual meetings.

The agenda and case list for the monthly meeting should be sent out seven days ahead of the meeting so that agencies can prepare accordingly.

d) Actions before the MARAC

The MARAC does not take away responsibility for immediate actions in relation to the safety of high risk victims from agencies involved, particularly with regard to statutory duties (e.g. police, children's services etc). Following a police call out or incident, there will be contact with the victim in advance of the meeting, normally through the IDVA service (DASU North Wales in Wrexham, Flintshire, Denbighshire and Conwy and Gorwel in Gwynedd and Anglesey).

Any immediate safeguarding concerns for the victim and/or children should be addressed prior to the meeting by the appropriate agencies and target hardening measures implemented. Any such action should be raised at the meeting to form part of the risk management plan.

e) Weekly MARAC meeting

The objective of weekly MARACs is to share RELEVANT information and to set safeguarding actions in a timely manner and avoid a wait of almost a month to hear a case in full.

Only core agencies are expected to attend weekly MARACs (Police, IDVA, Children's SSD, Adult SSD, probation, and health).

Additional agencies may attend but will not be routinely asked to contribute. The agenda will be circulated in advance, the request is that RELEVANT information is submitted to the administrative team in ADVANCE of the meeting.

The expectation is that each agency will research their own system and be asked to provide an update in the meeting. The information should be relevant and up to date.

The Chair will not routinely read through the entire agenda in the meeting.

The Chair will remind you of the confidentiality statement and will then review any incomplete actions.

The case numbers and victim details will be read out but then it will go straight to updates and relevant information.

Actions will be identified by members and summarised by the chair before moving onto the next case.

New cases will be listed first followed by the repeat cases at the end of the document.

If an agency sends a MARAC referral that requires clarity, the police will contact the referring agency to discuss and seek that clarity and agree jointly whether the case needs to be heard within MARAC.

If further discussion is required or additional agencies need to attend, then the case will be referred to monthly MARAC. It will be a group decision as to whether a case is escalated to monthly MARAC based on the risk and complexities identified

The health representative will be responsible for notifying the GP that the case is being heard at MARAC.

If an agency requires a legal aid letter that agency will complete the template on behalf of their own agency.

Meetings will be audio recorded by police and a copy saved using TEAMS software. Typed minutes for weekly MARAC will not be taken although agencies in attendance may record their own notes. An action tracker will be circulated following each weekly meeting.

f) Monthly MARAC meeting

Monthly MARAC is chaired by a NWP Detective Inspector. The agenda and case management documents will be shared with agencies 7 days in advance of the meeting, along with a TEAMS meeting link. The MARAC case document will include:

1. Details of any further incidents taking place since date of weekly meeting
2. Further DAO/agency updates since weekly MARAC
3. Weekly MARAC summary
4. Weekly MARAC actions

Typed minutes of the meeting will be circulated following the monthly meeting along with an associated action tracker.

g) Role of the Chair

NWP will chair weekly and monthly MARAC meetings and as such will help facilitate conversation and debate. The role of the Chair is not to singularly identify core actions nor be the sole decision maker. MARAC's are multi-agency forums to agree safety plans using the skill and experience of all partner agencies.

https://safelives.org.uk/sites/default/files/resources/MARAC%20Chair%20toolkit_0.doc

h) Information sharing

Referring agencies should always try and obtain consent from the victim before a referral is made to the MARAC. Since 25th May 2018 all agencies must be able to demonstrate that they are compliant with the General Data Protection Regulations (GDPR and 2020 GDPR UK) and accompanying Data Protection Act 2018 (DPA). Information shared must be **Necessary, Proportionate, Relevant, Adequate, Accurate, Timely and Secure**.

Appropriate policies must be in place. It is solely the responsibility of each agency to ensure compliance in terms of what and how information is shared and stored.

If consent has been declined, a referral should still be made to the MARAC due to the high risk nature. GDPR gives six lawful bases for sharing information and all six have equal status; no one basis is stronger or better than the other.

Consent from perpetrators is **NOT** required; **they are not informed about the MARAC**, as this could increase risk for the survivors and others in the household.

All MARACs should have an up to date Information Sharing Protocol, which conforms to the Wales Accord on Personal Information Sharing (WASPI). It is the responsibility of the local MARAC agencies to ensure the ISP remains current and this will be monitored by the Regional MARAC Steering Group.

i) Risk action Planning

A tailored action plan will be developed at the MARAC to increase the safety of the victim, children, perpetrator, other vulnerable parties and any professionals. Any actions given to an agency should be completed in a timely manner and any incomplete actions should be logged by the MARAC coordinator and addressed at the beginning of the next meeting.

j) Transfers

If the victim or perpetrator has moved out of area, the MARAC can agree to transfer the case to another appropriate MARAC. The MARAC Coordinator will forward all documentation to the police force in the new area. All partners will be expected to share relevant information with the receiving MARAC.

5) Equality

In order to ensure that the MARAC is fairly representing all groups within society the MARAC Coordinator collects information on the profile of all individuals referred to the MARAC. This information is monitored by the Regional MARAC/ADAPT Steering Group to identify whether those with protected characteristics are under /over represented.

6) Evaluation

MARAC data is collected, collated and reported to SafeLives by the MARAC Coordinator on a quarterly basis. Providing information to SafeLives enables North Wales' performance to be bench marked against other MARACs.

MARAC data is also analysed by the Regional MARAC/ADAPT Steering Group to identify good or poor performance and to identify any emerging trends. Identifying issues may lead to targeted improvement activity.

7) Withdrawal

If an organisation wishes to withdraw from the MARAC partnership then a letter should be sent to the Chair of the MARAC outlining the reasons for withdrawal.

8) Signatories

The following core agencies have read and agreed to the North Wales MARAC Operating Protocol:

Name	Agency	Confirm MARAC representative and deputy	Date	Signature



Wales Accord on the Sharing of Personal Information

Information Sharing Protocol for

Multi Agency Risk Assessment Conference (MARAC) – Conwy

Version **Reviewed** V 4.0 FINAL

Date Assured DECEMBER 2022

Quality Assurance Group North Wales QA Group

Contents

<i>1</i>	<i>Introduction to this ISP</i>	<i>2</i>
<i>2</i>	<i>The information sharing partner organisations</i>	<i>2</i>
<i>3</i>	<i>Specific organisational / practitioner obligations</i>	<i>4</i>
<i>4</i>	<i>Legislative / statutory powers</i>	<i>4</i>
<i>5</i>	<i>Personal information to be shared</i>	<i>8</i>
<i>6</i>	<i>Data Subjects' Rights</i>	<i>8</i>
<i>7</i>	<i>Information security</i>	<i>11</i>
<i>8</i>	<i>Review, Breaches and Termination of this Agreement</i>	<i>11</i>
<i>9</i>	<i>Appendix A – Glossary of Terms</i>	<i>12</i>
<i>10</i>	<i>Appendix B – Information Reference Table for Conwy Multi Agency Risk Assessment Conference (MARAC)</i>	<i>14</i>
<i>11</i>	<i>Appendix C – Partner Organisations Signatures</i>	<i>19</i>

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 dealing with high-risk cases of domestic abuse through the Multi Agency Risk Assessment Conference (MARAC) process in the Conwy area.
- 1.4 Personal information is shared to enable appropriate actions to be taken to increase public safety. The responsibility to take appropriate actions rests with individual agencies; it is not transferred to the MARAC. Personal information is shared for the following purpose:
 - To increase the safety, health and well-being of victims and their children;
 - To determine whether the perpetrator poses a significant risk to any particular individual or to the general community;
 - To construct jointly and implement a risk management plan that provides professional support to all those at risk and that reduces the risk of harm;
 - To reduce repeat victimisation;
 - To improve agency accountability; and
 - To improve support for staff involved in high risk Domestic Abuse cases.

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
North Wales Police	Detective Inspector, Crime Services Protecting Vulnerable Persons Unit	Protecting Vulnerable Persons Unit
Betsi Cadwaladr University Health Board	Associate Director of Safeguarding Assistant Director of Nursing Assistant Area Director Childrens Central	Safeguarding Substance Misuse Service Mental Health Team CAMHS

Conwy CBC	Head of Education Services	Education
	Head of Service – Children, Families & Safeguarding	Children's Services
	Head of Integrated Adult & Community Services	Adult Services
	Head of Regulatory & Housing Services	Regulatory and Housing Service
HMPPS (Probation Service in Wales)	Head of North Wales Probation Delivery Unit	North Wales Probation Delivery Unit
Aberconwy Domestic Abuse Service (ADAS)	Project Manager	Aberconwy Domestic Abuse Service
BAWSO	Head of Regional Services	North Wales
Adferiad	Safeguarding Lead	Safeguarding Lead MARAC reps
Domestic Abuse Safety Unit (DASU)	Senior Manager, Wrexham and Flintshire	Wrexham and Flintshire DASU
	Senior Manager, Conwy and Denbighshire	Conwy and Denbighshire DASU
Grwp Cynefin	Head of Communities	Housing
Kaleidoscope	Senior Resilience Worker	Conwy and Denbighshire
North Wales Women's Centre	Managing Director	North Wales Women's Centre Ltd
Relate Cymru	National Manager	Relate Cymru
Victim Support Cymru	Operations Manager	North Wales Victim Support
Wales and West Housing Association	Housing Officer	Housing
North Wales Housing	Communities Neighbourhood Officer	Housing

- 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
- 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
Necessary for compliance with a legal obligation – Art 6(1)(c)	☒ Social Services & Wellbeing (Wales) Act 2014 Part 7 – strengthens safeguarding responsibilities of organisations in relation to adults and children and the duty to report concerns. Part 9 requires local authorities to promote co-operation with relevant partners in relation to adults, children and carers and specifies arrangements for information sharing Local Authority, Registered Social Landlords

Task carried out in the public interest or in the exercise of official authority – Art 6(1)(e)	☒ Section 8 of the Data Protection Act 2018 Lawfulness of processing: public interest etc. In Article 6(1) of the UK GDPR (lawfulness of processing), the reference in point (e) to the processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority. 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. Relevant authorities include Police, Probation providers, Health, Local Authorities and Registered Social Landlords. The Offender Management Act Section 14 Disclosure for Offender Management Purposes <i>NWP, HMPPS, BCUHB</i>
Legitimate Interest – Art 6(1)(f)	☒ Legitimate Interest will be the lawful basis for processing of personal data for the MARAC process for the third sector partner organisations, where they cannot rely on the Social Services & Wellbeing Wales Act 2014, and aren't classed as Competent Authorities Consideration is given by each partner organisation to the three part test:- ▪ The purpose test ▪ The necessity test ▪ The balancing test <i>3rd Sector Partner Organisations</i>

Table 2 - Article 9 - Special Categories of Personal Data

Legal basis	Checkbox / Notes
Necessary for reasons of substantial public interest - Art 9(2)(g)	☒ Section 10 of the Data Protection Act 2018 Special Categories of personal data and criminal convictions 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. 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: Condition 10 – preventing or detecting unlawful acts Condition 18 - safeguarding of children and of individuals at risk <i>All partners other than NWP, HMPPS, BCUHB and Local authority</i>
Provision of preventative or occupational medicine, health or social care or treatment, or the	☒ Section 10 of the Data Protection Act 2018 Special Categories of personal data and criminal convictions

management of health or social care systems – Art 9(2)(h)	In Article 9(2) of the UK GDPR (Processing of special categories of data), the reference in point (h) that processing is necessary for the provision of health or social care BCUHB and Local authority
---	--

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	Processing is (select one): ☒ Carried out under the control of an official authority / competent authority NWP & HMPPS _____ and/or _____
	☒ Meets a relevant condition in Part 1, 2 or 3 of Schedule 1 of the Data Protection Act 2018. The relevant condition is: Schedule 1 Part 2 (10) preventing or detecting unlawful acts. All other partners

Table 4 - Competent authorities for Law Enforcement Purposes

Processing personal data for law enforcement purposes	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): ☐ 35(2)(a) The data subject has given consent. _____ or _____
	☒ 35(2)(b) The processing is necessary for the performance of a task carried out for that purpose by a competent authority. NWP and HMPPS
Sensitive processing / processing special categories of personal data for law enforcement purposes	[You should have already selected either 35(2)(a) or 35(2)(b) above] 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. The legal basis is (select one): ☐ 35(4) The data subject has given consent _____ or _____
	☒ 35(5) The processing is strictly necessary for the law enforcement purpose, and Meets a relevant condition in Schedule 8. The relevant condition is: Condition 1 – statutory etc purposes Condition 4 – safeguarding of children and individuals at risk NWP and HMPPS

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)	☒
Date of birth	☒
Address	☒
Postcode	☒
NHS number	☒
PNCID	☒

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
- 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	Comments
North Wales Police	Website ☒ Leaflet ☐ Form ☐ Verbal ☒ Other (specify in comments) ☐	https://www.north-wales.police.uk/accessing-information-1/data-protection/privacy-notice-2018	The referring organisation will provide the data subject with privacy information verbally
BCUHB	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://bcuhb.nhs.wales/use-of-site/privacy-policy/	
Conwy CBC	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://www.conwy.gov.uk/en/Council/Access-to-Information/Privacy-Notices/How-Conwy-County-Borough-Council-uses-your-Information.aspx	
HMPPS (National Probation Service in Wales)	Website ☐ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☒	 HMPPS Privacy Notice.pdf	Privacy Notice displayed in each offender waiting area.
Aberconwy Domestic Abuse Service	Website ☐ Leaflet ☒ Form ☐ Verbal ☒ Other (specify in comments) ☐		Privacy information is provided verbally at point of engagement with the client and a copy of our printed privacy statement is given to the subject if they wish.

BAWSO	Website	☐	https://bawso.org.uk/assets/Uploads/Bawso-Privacy-Policy.pdf	
Adferiad	Leaflet	☐		
	Form	☐		
	Verbal	☐	Privacy Policy - Adferiad Recovery	
	Other (specify in comments)	☐		
Domestic Abuse Safety Unit	Website	☒	https://www.dasunorthwales.co.uk/	
	Leaflet	☐		
Grwp Cynefin	Form	☐	http://www.grwpcynefin.org/en/about-us/policies/	
	Verbal	☐		
Kaleidoscope	Other (specify in comments)	☐	https://www.kaleidoscopeproject.org.uk/privacy-notice/	
North Wales Women's Centre	Website	☒	https://northwaleswomenscentre.com/privacy-policy	Clients are asked to complete an enrolment form which contains Privacy information, and they are also directed to the website
	Leaflet	☐		
	Form	☒		
	Verbal	☐		
	Other (specify in comments)	☐		
Relate Cymru	Website	☒	https://www.relate.org.uk/cymru/privacy	
	Leaflet	☐		
	Form	☐		
	Verbal	☐		
	Other (specify in comments)	☐		
Victim Support	Website	☒	 Full Service Delivery Fair Processing Notice	Privacy information provided using website, letter and also verbal.
	Leaflet	☒		
	Form	☐		
	Verbal	☒		
	Other (specify in comments)	☐		
Wales and West Housing Association	Website	☒	https://www.wwha.co.uk/en/legal/	
	Leaflet	☐		
	Form	☐		
North Wales Housing	Verbal	☐	Data Protection – North Wales Housing (nwaha.org.uk)	
	Other (specify in comments)	☐		

--	--	--	--

- 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 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 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.

9 Appendix A – Glossary of Terms

Term	Definition
Data Protection Act 2018	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. The 2018 Act also transposes EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law. It is important the UK 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 UK 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.
UK GDPR	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.
Law Enforcement Purposes	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)
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 data about criminal convictions, offences or related security measures	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))
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.' (UK GDPR Art 4(2))
Special categories of data / sensitive processing	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))
PNCID	This relates to the Police National Computer Identification number, allocated to an individual when entered on PNC.

10 **Appendix B – Information Reference Table for Conwy Multi Agency Risk Assessment Conference (MARAC)**

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	001 – Referral	002 – Assessment and Allocation	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
1	Information exchange <i>General description of the process or stage to which the information sharing relates.</i>	Referral of potential MARAC case by any organisation/agency	Assessment undertaken by NWP Protecting Vulnerable Persons Unit by collecting further information from agencies other than the referring agency, and allocation of cases to be discussed at monthly MARAC	Discussion of cases at MARAC to identify risks posed to Service User, assess the needs of the Service User, agree and allocate the provision of appropriate services and review the provision of agreed services from previous meetings	NWP document minutes and actions from meeting and updates of intervention, and circulate to all partner organisations

2	What information will be shared? <i>Describe the information to be shared – you do not need to go to ‘field level’ detail.</i> <u>Please note: Only the minimum and relevant personal information is to be shared and strictly on a case by case basis.</u>	MARAC referrals may contain any or all of the following Personal identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal Identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal Identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status Details discussed at the MARAC meeting
---	--	--	---	---	---

3	Description	001 – Referral		002 – Assessment and Allocation		003 – discussion at MARAC meeting and allocation of intervention		004 – distribution of minutes and actions	
		Who by	Who to	Who by	Who to	Who by	Who to	Who by	Who to
3	Partner Organisation(s) <i>Details of provider and recipient organisation(s)</i> <i>Ensure the organisations listed reflect section 2 of the ISP i.e. are all organisations listed in section 2</i>	North Wales Police	North Wales Police	North Wales Police	North Wales Police	North Wales Police	North Wales Police	North Wales Police	North Wales Police
		Betsi Cadwaladr UHB		Betsi Cadwaladr UHB		Betsi Cadwaladr UHB	Betsi Cadwaladr UHB		Betsi Cadwaladr UHB
		Conwy CBC		Conwy CBC		Conwy CBC	Conwy CBC		Conwy CBC
		HMPPS		HMPPS		HMPPS	HMPPS		HMPPS
		Aberconwy Domestic Abuse Service		Aberconwy Domestic Abuse Service		Aberconwy Domestic Abuse Service	Aberconwy Domestic Abuse Service		Aberconwy Domestic Abuse Service
		BAWSO		BAWSO		BAWSO	BAWSO		BAWSO
		Adferiad		Adferiad		Adferiad	Adferiad		Adferiad
		Domestic Abuse Safety Unit		Domestic Abuse Safety Unit		Domestic Abuse Safety Unit	Domestic Abuse Safety Unit		Domestic Abuse Safety Unit
		Grwp Cynefin		Grwp Cynefin		Grwp Cynefin	Grwp Cynefin		Grwp Cynefin
		Kaleidoscope		Kaleidoscope		Kaleidoscope	Kaleidoscope		Kaleidoscope
		North Wales Women's Centre		North Wales Women's Centre		North Wales Women's Centre	North Wales Women's Centre		North Wales Women's Centre
		Relate Cymru		Relate Cymru		Relate Cymru	Relate Cymru		Relate Cymru
		Victim Support		Victim Support		Victim Support	Victim Support		Victim Support
		Wales & West Housing		Wales & West Housing		Wales & West Housing	Wales & West Housing		Wales & West Housing
		North Wales Housing Association		North Wales Housing Association		North Wales Housing Association	North Wales Housing Association		North Wales Housing Association

	Description	001 – Referral	002 – Assessment and Allocation	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
4	How is information shared and what methods are used to keep the information secure? <i>Provide, in detail the specific agreed secure methods for sharing personal information</i>	Secure email, either using TLS1.2 or encrypted email	Secure email, either using TLS1.2 or encrypted email	Face to face meeting or secure online meeting (Microsoft Teams)	Minutes and actions sent out using Secure email, either using TLS1.2 or encrypted email
5	Reliance on consent <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>	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent

	Description	001 – Referral	002 – Assessment and Allocation	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
6	Notes for Practitioners		Note: Although the schools are not partners to the MARAC process, they may be approached by the Education Welfare Officer to provide appropriate information as part of the research process prior to the MARAC.	Any printed documents or notes made during meeting must be securely destroyed	Note: Following each monthly MARAC meeting the MARAC Administrator forwards the minutes to all MARAC partners, along with an Action Tracker. These partners are then required to feedback on completed actions or those outstanding to the Public Protection Detective Sergeant, who will note them on subsequent minutes of the next MARAC meeting for discussion as appropriate. Following each weekly MARAC meeting, the MARAC administrator sends an Action Tracker to all partners, as above.

11 Appendix C – Partner Organisations Signatures

This section should only be completed once the ISP has been assured by a Quality Assurance group. Further information on the ISP development process can be found on the WASPI Website.

By signing below, partner organisations are confirming they agree with the content of the ISP. In the context of sharing personal information, signing the ISP is one way to demonstrate accountability with the principles set out in Article 5 of UK GDPR.

The signatory will be an appropriate person with authority to sign the ISP on behalf of the organisation. The ISP lead has responsibility for obtaining signatures to the ISP.

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	



Wales Accord on the Sharing of Personal Information

Information Sharing Protocol for

Multi Agency Risk Assessment Conference (MARAC) – Denbighshire

Version **Reviewed** V4.0 FINAL

Date Assured December 2022

Quality Assurance Group North Wales QA Group

Contents

<i>1</i>	<i>Introduction to this ISP</i>	<i>2</i>
<i>2</i>	<i>The information sharing partner organisations</i>	<i>2</i>
<i>3</i>	<i>Specific organisational / practitioner obligations</i>	<i>3</i>
<i>4</i>	<i>Legislative / statutory powers</i>	<i>4</i>
<i>5</i>	<i>Personal information to be shared</i>	<i>7</i>
<i>6</i>	<i>Data Subjects' Rights</i>	<i>8</i>
<i>7</i>	<i>Information security</i>	<i>11</i>
<i>8</i>	<i>Review, Breaches and Termination of this Agreement</i>	<i>11</i>
<i>9</i>	<i>Appendix A – Glossary of Terms</i>	<i>12</i>
<i>10</i>	<i>Appendix B – Information Reference Table for Denbighshire Multi Agency Risk Assessment Conference (MARAC)</i>	<i>14</i>
<i>11</i>	<i>Appendix C – Partner Organisations Signatures</i>	<i>19</i>

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 dealing with high-risk cases of domestic abuse through the Multi Agency Risk Assessment Conference (MARAC) process in the Denbighshire area.
- 1.4 Personal information is shared to enable appropriate actions to be taken to increase public safety. The responsibility to take appropriate actions rests with individual agencies; it is not transferred to the MARAC. Personal information is shared for the following purpose:
 - To increase the safety, health and well-being of victims and their children;
 - To determine whether the perpetrator poses a significant risk to any particular individual or to the general community;
 - To construct jointly and implement a risk management plan that provides professional support to all those at risk and that reduces the risk of harm;
 - To reduce repeat victimisation;
 - To improve agency accountability; and
 - To improve support for staff involved in high risk Domestic Abuse cases.

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
North Wales Police	Detective Inspector, Crime Services Protecting Vulnerable Persons Unit	Protecting Vulnerable Persons Unit
Betsi Cadwaladr University Health Board	Associate Director of Safeguarding Assistant Director of Nursing Assistant Area Director Childrens Central	Safeguarding Substance Misuse Service Mental Health Team CAMHS

Denbighshire CC	Lead Officer – Community Housing	Housing
	Head of Children and Family Services	Education Children's Services Single Care Pathway Youth Justice Services
	Head of Community Support Services	Adult Services
HMPPS (Probation Service in Wales)	Head of North Wales Probation Delivery Unit	North Wales Probation Delivery Unit
BAWSO	Head of Regional Services	North Wales
ADFERIAD	Safeguarding Lead	Safeguarding Lead MARAC reps
Domestic Abuse Safety Unit (DASU)	Senior Manager, Wrexham and Flintshire	Wrexham and Flintshire DASU
	Senior Manager, Conwy and Denbighshire	Conwy and Denbighshire DASU
Grwp Cynefin	Head of Communities	Housing
Kaleidoscope	Senior Resilience Worker	Conwy and Denbighshire
North Wales Women's Centre	Managing Director	North Wales Women's Centre Ltd
Relate Cymru	National Manager	Relate Cymru
Victim Support	Operations Manager	North Wales Victim Support
Wales and West Housing Association	Housing Officer	Housing
North Wales Housing Association	Communities Neighbourhood Officer	Housing

- 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
- 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
Necessary for compliance with a legal obligation – Art 6(1)(c)	☒ Social Services & Wellbeing (Wales) Act 2014 Part 7 – strengthens safeguarding responsibilities of organisations in relation to adults and children and the duty to report concerns. Part 9 requires local authorities to promote co-operation with relevant partners in relation to adults, children and carers and specifies arrangements for information sharing Local Authority, Registered Social Landlords
Task carried out in the public interest or in the exercise of official authority – Art 6(1)(e)	☒ Section 8 of the Data Protection Act 2018 Lawfulness of processing: public interest etc. In Article 6(1) of the UK GDPR (lawfulness of processing), the reference in point (e) to the processing of personal data that is

	necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority 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. Relevant authorities include Police, Probation providers, Health, Local Authorities and Registered Social Landlords. The Offender Management Act Section 14 Disclosure for Offender Management Purposes <i>NWP, HMPPS, BCUHB</i>
Legitimate Interest – Art 6(1)(f)	☒ Legitimate Interest will be the lawful basis for processing of personal data for the MARAC process for the third sector partner organisations, where they cannot rely on the Social Services & Wellbeing Wales Act 2014, and aren't classed as Competent Authorities Consideration is given by each partner organisation to the three part test:- ▪ The purpose test ▪ The necessity test ▪ The balancing test <i>3rd Sector Partner Organisations</i>

Table 2 - Article 9 - Special Categories of Personal Data

Legal basis	Checkbox / Notes
Necessary for reasons of substantial public interest - Art 9(2)(g)	☒ Section 10 of the Data Protection Act 2018 Special Categories of personal data and criminal convictions 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. 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: Condition 10 – preventing or detecting unlawful acts Condition 18 - safeguarding of children and of individuals at risk <i>All partners other than NWP, HMPPS, BCUHB and Local authority</i>
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)	☒ Section 10 of the Data Protection Act 2018 Special Categories of personal data and criminal convictions In Article 9(2) of the UK GDPR (Processing of special categories of data), the reference in point (h) that processing is necessary for the provision of health or social care <i>BCUHB and Local authority</i>

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	Processing is (select one): ☒ Carried out under the control of an official authority / competent authority NWP & HMPPS _____ and/or _____
	☒ Meets a relevant condition in Part 1, 2 or 3 of Schedule 1 of the Data Protection Act 2018. The relevant condition is: Schedule 1 Part 2 (10) preventing or detecting unlawful acts. All other partners

Table 4 - Competent authorities for Law Enforcement Purposes

Processing personal data for law enforcement purposes	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): ☐ 35(2)(a) The data subject has given consent. _____ or _____
	☒ 35(2)(b) The processing is necessary for the performance of a task carried out for that purpose by a competent authority. NWP and HMPPS
Sensitive processing / processing special categories of personal data for law enforcement purposes	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. The legal basis is (select one): ☐ 35(4) The data subject has given consent _____ or _____
	☒ 35(5) The processing is strictly necessary for the law enforcement purpose, and Meets a relevant condition in Schedule 8. The relevant condition is: Condition 1 – statutory etc purposes Condition 4 – safeguarding of children and individuals at risk NWP and HMPPS

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)	☒
Date of birth	☒
Address	☒
Postcode	☒
NHS number	☒
PNCID	☒

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
- 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	Comments
	Website ☒		

North Wales Police	Leaflet ☐ Form ☐ Verbal ☒ Other (specify in comments) ☐	https://www.north-wales.police.uk/accessing-information-1/data-protection/privacy-notice-2018	The referring organisation will provide the data subject with privacy information verbally
BCUHB	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://bcuhb.nhs.wales/use-of-site/privacy-policy/	
Denbighshire CC	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://www.denbighshire.gov.uk/privacy https://www.sirddinbych.gov.uk/preifatrwydd	
HMPPS	Website ☐ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☒	 HMPPS Privacy Notice.pdf	Privacy Notice displayed in each offender waiting area.
BAWSO Adferiad	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://bawso.org.uk/assets/Uploads/Bawso-Privacy-Policy.pdf Privacy Policy - Adferiad Recovery	
Domestic Abuse Safety Unit	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://www.dasunorthwales.co.uk/	
Grwp Cynefin Kaleidoscope	Website ☒ Leaflet ☐ Form ☐	http://www.grwpcynefin.org/en/about-us/policies/	

	Verbal ☐	https://www.kaleidoscopeproject.org.uk/privacy-notice/	
	Other (specify in comments) ☐		
North Wales Women's Centre	Website ☒ Leaflet ☐ Form ☒ Verbal ☐ Other (specify in comments) ☐	https://northwaleswomenscentre.com/privacy-policy	Clients are asked to complete an enrolment form which contains Privacy information, and they are also directed to the website
Relate Cymru	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://www.relate.org.uk/cymru/privacy	
Victim Support	Website ☒ Leaflet ☒ Form ☐ Verbal ☒ Other (specify in comments) ☐	 Full Service Delivery Fair Processing Notice	Privacy information provided using website, letter and also verbal.
Wales and West Housing Association	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://www.wwha.co.uk/en/legal/	
North Wales Housing Association	Other (specify in comments) ☐	Data Protection – North Wales Housing (nwaha.org.uk)	

- 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 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 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.

9 Appendix A – Glossary of Terms

Term	Definition
Data Protection Act 2018	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. The 2018 Act also transposes EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law. It is important the UK 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 UK 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.
UK GDPR	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.
Law Enforcement Purposes	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)
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 data about criminal convictions, offences or related security measures	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))
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.' (UK GDPR Art 4(2))
Special categories of data / sensitive processing	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))
PNCID	This relates to the Police National Computer Identification number, allocated to an individual when entered on PNC.

10 **Appendix B – Information Reference Table for Denbighshire Multi Agency Risk Assessment Conference (MARAC)**

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	001 – Referral	002 – Assessment and Allocation to MARAC	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
1	Information exchange <i>General description of the process or stage to which the information sharing relates.</i>	Referral of potential MARAC case by any organisation/agency	Assessment undertaken by NWP Protecting Vulnerable Persons Unit by collecting further information from agencies other than the referring agency, and allocation of cases to be discussed at monthly MARAC	Discussion of cases at MARAC to identify risks posed to Service User, assess the needs of the Service User, agree and allocate the provision of appropriate services and review the provision of agreed services from previous meetings	NWP document minutes and actions from meeting and updates of intervention, and circulate to all partner organisations

2	What information will be shared? <i>Describe the information to be shared – you do not need to go to ‘field level’ detail.</i> <u>Please note: Only the minimum and relevant personal information is to be shared and strictly on a case by case basis.</u>	MARAC referrals may contain any or all of the following Personal identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status Details discussed at the MARAC meeting and actions allocated
---	--	--	---	---	---

3	Description	001 – Referral		002 – Assessment and Allocation to MARAC		003 – discussion at MARAC meeting and allocation of intervention		004 – distribution of minutes and actions	
		Who by	Who to	Who by	Who to	Who by	Who to	Who by	Who to
	Partner Organisation(s) <i>Details of provider and recipient organisation(s)</i> <i>Ensure the organisations listed reflect section 2 of the ISP i.e. are all organisations listed in section 2</i>	North Wales Police Betsi Cadwaladr UHB Denbighshire CC HMPPS BAWSO Adferiad Domestic Abuse Safety Unit (DASU) Grwp Cynefin Kaleidoscope North Wales Women's Centre Relate Cymru Victim Support Wales and West Housing Association North Wales Housing association	North Wales Police	North Wales Police Betsi Cadwaladr UHB Denbighshire CC HMPPS BAWSO Adferiad Domestic Abuse Safety Unit (DASU) Grwp Cynefin Kaleidoscope North Wales Women's Centre Relate Cymru Victim Support Wales and West Housing Association North Wales Housing association	North Wales Police	North Wales Police Betsi Cadwaladr UHB Denbighshire CC HMPPS BAWSO Adferiad Domestic Abuse Safety Unit (DASU) Grwp Cynefin Kaleidoscope North Wales Women's Centre Relate Cymru Victim Support Wales and West Housing Association North Wales Housing association	North Wales Police Betsi Cadwaladr UHB Denbighshire CC HMPPS BAWSO Adferiad Domestic Abuse Safety Unit (DASU) Grwp Cynefin Kaleidoscope North Wales Women's Centre Relate Cymru Victim Support Wales and West Housing Association North Wales Housing association	North Wales Police	North Wales Police Betsi Cadwaladr UHB Denbighshire CC HMPPS BAWSO Adferiad Domestic Abuse Safety Unit (DASU) Grwp Cynefin Kaleidoscope North Wales Women's Centre Relate Cymru Victim Support Wales and West Housing Association North Wales Housing association

	Description	001 – Referral	002 – Assessment and Allocation to MARAC	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
4	How is information shared and what methods are used to keep the information secure? <i>Provide, in detail the specific agreed secure methods for sharing personal information</i>	Secure email, either using TLS1.2 or encrypted email	Secure email, either using TLS1.2 or encrypted email	Face to face meeting or secure online meeting (Microsoft Teams)	Minutes and actions sent out using Secure email, either using TLS1.2 or encrypted email
5	Reliance on consent <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>	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent

	Description	001 – Referral	002 – Assessment and Allocation to MARAC	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
6	Notes for Practitioners		Note: Although the schools are not partners to the MARAC process, they may be approached by the Education Welfare Officer to provide appropriate information as part of the research process prior to the MARAC.	Any printed documents or notes made during meeting must be securely destroyed	Note: Following each monthly MARAC meeting the MARAC Administrator forwards the minutes to all MARAC partners, along with an Action Tracker. These partners are then required to feedback on completed actions or those outstanding to the Public Protection Detective Sergeant, who will note them on subsequent minutes of the next MARAC meeting for discussion as appropriate. Following each weekly MARAC meeting, the MARAC administrator sends an Action Tracker to all partners, as above.

11 Appendix C – Partner Organisations Signatures

This section should only be completed once the ISP has been assured by a Quality Assurance group. Further information on the ISP development process can be found on the WASPI Website.

By signing below, partner organisations are confirming they agree with the content of the ISP. In the context of sharing personal information, signing the ISP is one way to demonstrate accountability with the principles set out in Article 5 of UK GDPR.

The signatory will be an appropriate person with authority to sign the ISP on behalf of the organisation. The ISP lead has responsibility for obtaining signatures to the ISP.

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	



Wales Accord on the Sharing of Personal Information

Multi Agency Risk Assessment Conference
(MARAC) – Flintshire

Information Sharing Protocol for

Version **Reviewed** V 4.0 FINAL

Date Assured December 2022

Quality Assurance Group North Wales QA Group

Contents

1	<i>Introduction to this ISP</i>	2
2	<i>The information sharing partner organisations</i>	2
3	<i>Specific organisational / practitioner obligations</i>	4
4	<i>Legislative / statutory powers</i>	4
5	<i>Personal information to be shared</i>	8
6	<i>Data Subjects' Rights</i>	8
7	<i>Information security</i>	11
8	<i>Review, Breaches and Termination of this Agreement</i>	12
9	<i>Appendix A – Glossary of Terms</i>	13
10	<i>Appendix B – Information Reference Table for Multi Agency Risk Assessment Conference (MARAC)</i>	15
11	<i>Appendix C – Partner Organisations Signatures</i>	20

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 dealing with high-risk cases of domestic abuse through the Multi Agency Risk Assessment Conference (MARAC) process in the Flintshire area.
- 1.4 Personal information is shared to enable appropriate actions to be taken to increase public safety. The responsibility to take appropriate actions rests with individual agencies; it is not transferred to the MARAC. Personal information is shared for the following purpose:
 - To increase the safety, health and well-being of victims and their children;
 - To determine whether the perpetrator poses a significant risk to any particular individual or to the general community;
 - To construct jointly and implement a risk management plan that provides professional support to all those at risk and that reduces the risk of harm;
 - To reduce repeat victimisation;
 - To improve agency accountability; and
 - To improve support for staff involved in high risk Domestic Abuse cases.

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
North Wales Police	Detective Inspector, Crime Services Protecting Vulnerable Persons Unit	Protecting Vulnerable Persons Unit
Betsi Cadwaladr University Health Board	Associate Director of Safeguarding Assistant Director of Nursing Assistant Area Director Childrens Central	Safeguarding Substance Misuse Service Mental Health Team CAMHS

Flintshire CC	Senior Manager, Inclusion and Progression	Education
	Housing and Prevention Service Manager	Housing
	Senior Manager, Children, Social Services	Children's Services
	Senior Manager, Integrated Services, Lead Adults	Adult Social Care
	Community and Business Protection Manager	Environment/Community Safety
	Senior Manager, Integrated Youth Provision	Youth Justice Services
HMPPS (Probation Service in Wales)	Head of North Wales Probation Delivery Unit	Head of North Wales Probation Delivery Unit
BAWSO	Head of Regional Services	North Wales
Adferiad	Safeguarding Lead	Safeguarding Lead MARAC reps
Clwyd Alyn Housing Association	Director of Care and Support	Care and Support
	Operations Manager	Women's Aid
Domestic Abuse Safety Unit (DASU)	Senior Manager, Wrexham and Flintshire	Wrexham and Flintshire DASU
	Senior Manager, Conwy and Denbighshire	Conwy and Denbighshire DASU
Relate Cymru	National Manager	Relate Cymru
Victim Support	Deputy Service Director	North Wales Victim Support
Wales and West Housing Association	Housing Manager	Housing
Grwp Cynefin Housing	Head of Communities	Housing

- 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
- 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
-------------	-------------------

Necessary for compliance with a legal obligation – Art 6(1)(c)	☒ Social Services & Wellbeing (Wales) Act 2014 Part 7 – strengthens safeguarding responsibilities of organisations in relation to adults and children and the duty to report concerns. Part 9 requires local authorities to promote co-operation with relevant partners in relation to adults, children and carers and specifies arrangements for information sharing Local Authority, Registered Social Landlords
Task carried out in the public interest or in the exercise of official authority – Art 6(1)(e)	☒ Section 8 of the Data Protection Act 2018 Lawfulness of processing: public interest etc. In Article 6(1) of the UK GDPR (lawfulness of processing), the reference in point (e) to the processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority. 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. Relevant authorities include Police, Probation providers, Health, Local Authorities and Registered Social Landlords. The Offender Management Act Section 14 Disclosure for Offender Management Purposes NWP, HMPPS, BCUHB
Legitimate Interest – Art 6(1)(f)	☒ Legitimate Interest will be the lawful basis for processing of personal data for the MARAC process for the third sector partner organisations, where they cannot rely on the Social Services & Wellbeing Wales Act 2014, and aren't classed as Competent Authorities Consideration is given by each partner organisation to the three part test:- ▪ The purpose test ▪ The necessity test ▪ The balancing test 3rd Sector Partner Organisations

Table 2 - Article 9 - Special Categories of Personal Data

Legal basis	Checkbox / Notes
Necessary for reasons of substantial public interest - Art 9(2)(g)	☒ Section 10 of the Data Protection Act 2018 Special Categories of personal data and criminal convictions 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. 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: Condition 10 – preventing or detecting unlawful acts

	Condition 18 - safeguarding of children and of individuals at risk All partners other than NWP, HMPPS, BCUHB and Local authority
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)	☒ Section 10 of the Data Protection Act 2018 Special Categories of personal data and criminal convictions In Article 9(2) of the UK GDPR (Processing of special categories of data), the reference in point (h) that processing is necessary for the provision of health or social care BCUHB and Local authority

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	Processing is (select one): ☒ Carried out under the control of an official authority / competent authority NWP & HMPPS _____ and/or _____
	☒ Meets a relevant condition in Part 1, 2 or 3 of Schedule 1 of the Data Protection Act 2018. The relevant condition is: Schedule 1 Part 2 (10) preventing or detecting unlawful acts. All other partners

Table 4 - Competent authorities for Law Enforcement Purposes

Processing personal data for law enforcement purposes	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): ☐ 35(2)(a) The data subject has given consent. _____ or _____
	☒ 35(2)(b) The processing is necessary for the performance of a task carried out for that purpose by a competent authority. NWP and HMPPS

Sensitive processing / processing special categories of personal data for law enforcement purposes	<i>[You should have already selected either 35(2)(a) or 35(2)(b) above]</i> 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. The legal basis is (select one): ☐ 35(4) The data subject has given consent
	☒ 35(5) The processing is strictly necessary for the law enforcement purpose, and Meets a relevant condition in Schedule 8. The relevant condition is: Condition 1 – statutory etc purposes Condition 4 – safeguarding of children and individuals at risk NWP and HMPPS

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)	☒
Date of birth	☒
Address	☒
Postcode	☒
NHS number	☒
PNCID	☒

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

- 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	Comments
North Wales Police	Website ☒ Leaflet ☐ Form ☐ Verbal ☒ Other (specify in comments) ☐	https://www.north-wales.police.uk/accessing-information-1/data-protection/privacy-notice-2018	The referring organisation will provide the data subject with privacy information verbally
BCUHB	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://bcuhb.nhs.wales/use-of-site/privacy-policy/	
Flintshire CC	Website ☒ Leaflet ☒ Form ☒ Verbal ☐ Other (specify in comments) ☐	https://www.flintshire.gov.uk/en/Resident/Contact-Us/Privacy-Notice.aspx  Childrens Privacy Notice version 2 wag	Social Services provide our Privacy Notices at first point of contact, such as when a referral is made we have telephone PN on our Children's services switchboard system, we then provide Privacy Notices throughout

		 Adults Privacy Notice.docx	the care journey, when any personal sensitive information is collected. All assessments/ forms have our PN attached to inform the individual of how we process their information. We also provide a web link to the councils over all PN if needed.
HMPPS	Website ☐ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☒	 HMPPS Privacy Notice.pdf	Privacy Notice displayed in each offender waiting area.
BAWSO Adferiad Clwyd Alyn Housing Association	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://bawso.org.uk/assets/Uploads/Bawso-Privacy-Policy.pdf Privacy Policy - Adferiad Recovery Privacy Policy : ClwydAlyn Housing	
Domestic Abuse Safety Unit	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://www.dasunorthwales.co.uk/	
Relate Cymru	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://www.relate.org.uk/cymru/privacy	

Victim Support	Website ☒ Leaflet ☒ Form ☐ Verbal ☒ Other (specify in comments) ☐	 Full Service Delivery Fair Processing Notice	Privacy information provided using website, letter and also verbal.
Wales and West Housing Association	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://www.wwha.co.uk/en/legal/	
Grwp Cynefin Housing	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐ ☐	Privacy GDPR - Grŵp Cynefin (grwpcynefin.org)	

- 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 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 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
Appropriate Policy Document	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. 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.
Data Protection Act 2018	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. The 2018 Act also transposes EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law. It is important the UK 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 UK 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.
UK GDPR	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.
Law Enforcement Purposes	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)
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 data about criminal convictions, offences or related security measures	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))
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.' (UK GDPR Art 4(2))
Special categories of data / sensitive processing	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))
PNCID	This relates to the Police National Computer Identification number, allocated to an individual when entered on PNC.

10 **Appendix B – Information Reference Table for Flintshire Multi Agency Risk Assessment Conference (MARAC)**

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	001 – Referral	002 – Assessment and Allocation	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
1	Information exchange <i>General description of the process or stage to which the information sharing relates.</i>	Referral of potential MARAC case by any organisation/agency	Assessment undertaken by NWP Protecting Vulnerable Persons Unit by collecting further information from agencies other than the referring agency, and allocation of cases to be discussed at monthly MARAC	Discussion of cases at MARAC to identify risks posed to Service User, assess the needs of the Service User, agree and allocate the provision of appropriate services and review the provision of agreed services from previous meetings	NWP document minutes and actions from meeting and updates of intervention, and circulate to all partner organisations

2	What information will be shared? <i>Describe the information to be shared – you do not need to go to ‘field level’ detail.</i> <u>Please note: Only the minimum and relevant personal information is to be shared and strictly on a case by case basis.</u>	MARAC referrals may contain any or all of the following:- Personal identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal Identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal Identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status Details discussed at the MARAC meeting
---	--	--	---	---	---

3	Description	001 – Referral		002 – Assessment and Allocation		003 – discussion at MARAC meeting and allocation of intervention		004 – distribution of minutes and actions	
		Who by	Who to	Who by	Who to	Who by	Who to	Who by	Who to
	Partner Organisation(s) <i>Details of provider and recipient organisation(s)</i> <i>Ensure the organisations listed reflect section 2 of the ISP i.e. are all organisations listed in section 2</i>	North Wales Police Betsi Cadwaladr UHB Flintshire CC HMPPS BAWSO Adferiad Clwyd Alyn Housing Association Domestic Abuse Safety Unit Relate Cymru Victim Support Wales and West Housing Grwp Cynefin Housing	North Wales Police	North Wales Police Betsi Cadwaladr UHB Flintshire CC HMPPS BAWSO Adferiad Clwyd Alyn Housing Association Domestic Abuse Safety Unit Relate Cymru Victim Support Wales and West Housing Grwp Cynefin Housing	North Wales Police	North Wales Police Betsi Cadwaladr UHB Flintshire CC HMPPS BAWSO Adferiad Clwyd Alyn Housing Association Domestic Abuse Safety Unit Relate Cymru Victim Support Wales and West Housing Grwp Cynefin Housing	North Wales Police Betsi Cadwaladr UHB Flintshire CC HMPPS BAWSO Adferiad Clwyd Alyn Housing Association Domestic Abuse Safety Unit Relate Cymru Victim Support Wales and West Housing Grwp Cynefin Housing	North Wales Police	North Wales Police Betsi Cadwaladr UHB Flintshire CC HMPPS BAWSO Adferiad Clwyd Alyn Housing Association Domestic Abuse Safety Unit Relate Cymru Victim Support Wales and West Housing Grwp Cynefin Housing

	Description	001 – Referral	002 – Assessment and Allocation	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
4	How is information shared and what methods are used to keep the information secure? <i>Provide, in detail the specific agreed secure methods for sharing personal information</i>	Secure email, either using TLS1.2 or encrypted email	Secure email, either using TLS1.2 or encrypted email	Face to face meeting or secure online meeting (Microsoft Teams)	Minutes and actions sent out using Secure email, either using TLS1.2 or encrypted email
5	Reliance on consent <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>	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent

	Description	001 – Referral	002 – Assessment and Allocation	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
6	Notes for Practitioners		Note: Although the schools are not partners to the MARAC process, they may be approached by the Education Welfare Officer to provide appropriate information as part of the research process prior to the MARAC.	Any printed documents or notes made during meeting must be securely destroyed	Note: Following each monthly MARAC meeting the MARAC Administrator forwards the minutes to all MARAC partners, along with an Action Tracker. These partners are then required to feedback on completed actions or those outstanding to the Public Protection Detective Sergeant, who will note them on subsequent minutes of the next MARAC meeting for discussion as appropriate. Following each weekly MARAC meeting, the MARAC administrator sends an Action Tracker to all partners, as above.

11 Appendix C – Partner Organisations Signatures

This section should only be completed once the ISP has been assured by a Quality Assurance group. Further information on the ISP development process can be found on the WASPI Website.

By signing below, partner organisations are confirming they agree with the content of the ISP. In the context of sharing personal information, signing the ISP is one way to demonstrate accountability with the principles set out in Article 5 of UK GDPR.

The signatory will be an appropriate person with authority to sign the ISP on behalf of the organisation. The ISP lead has responsibility for obtaining signatures to the ISP.

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	



Wales Accord on the Sharing of Personal Information

Information Sharing Protocol for Multi Agency Risk Assessment Conference (MARAC) - Gwynedd

Version **Reviewed** V4.0 FINAL

Date Assured December 2022

Quality Assurance Group North Wales QA Group

Contents

1	<i>Introduction to this ISP</i>	3
2	<i>The information sharing partner organisations</i>	3
3	<i>Specific organisational / practitioner obligations</i>	4
4	<i>Legislative / statutory powers</i>	5
5	<i>Personal information to be shared</i>	8
6	<i>Data Subjects' Rights</i>	9
7	<i>Information security</i>	11
8	<i>Review, Breaches and Termination of this Agreement</i>	11
9	<i>Appendix A – Glossary of Terms</i>	12
10	<i>Appendix B – Information Reference Table for Gwynedd Multi Agency Risk Assessment Conference (MARAC)</i>	14
11	<i>Appendix C – Partner Organisations Signatures</i>	19

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 dealing with high-risk cases of domestic abuse through the Multi Agency Risk Assessment Conference (MARAC) process in the Gwynedd area.
- 1.4 Personal information is shared to enable appropriate actions to be taken to increase public safety. The responsibility to take appropriate actions rests with individual agencies; it is not transferred to the MARAC. Personal information is shared for the following purpose:
 - To increase the safety, health and well-being of victims and their children;
 - To determine whether the perpetrator poses a significant risk to any particular individual or to the general community;
 - To construct jointly and implement a risk management plan that provides professional support to all those at risk and that reduces the risk of harm;
 - To reduce repeat victimisation;
 - To improve agency accountability; and
 - To improve support for staff involved in high risk Domestic Abuse cases.

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
North Wales Police	Detective Inspector, Crime Services Protecting Vulnerable Persons Unit	Protecting Vulnerable Persons Unit
Betsi Cadwaladr University Health Board	Associate Director of Safeguarding Assistant Director of Nursing Assistant Area Director Childrens Central	Safeguarding Substance Misuse Service Mental Health Team CAMHS
Gwynedd County Council	Senior Safeguarding Children's Officer	Education

	Senior Operational Manager Adult Safeguarding Co-ordinator Assistant Head – Housing and Well-being	Children's Services Adult Services Housing
Youth Justice Service (Gwynedd ac Ynys Mon)	Service Manager	Youth Justice Service
HMPPS (Probation Service in Wales)	Head of North Wales Probation Delivery Unit	North Wales Probation Delivery Unit
ADRA	Director of Customers and Communities	Customers and Communities
ADFERIAD	Service Manager	ADFERIAD
Grwp Cynefin	Head of Neighbourhoods	Operations
North Wales Housing Association	Director of Operations	North Wales Housing
BAWSO	Head of Regional Services	North Wales
Gorwel	IDVA Team Leader/Safeguarding	IDVA team

- 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
- 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
Necessary for compliance with a legal obligation – Art 6(1)(c)	☒ Social Services & Wellbeing (Wales) Act 2014 Part 7 – strengthens safeguarding responsibilities of organisations in relation to adults and children and the duty to report concerns. Part 9 requires local authorities to promote co-operation with relevant partners in relation to adults, children and carers and specifies arrangements for information sharing Local Authority, Registered Social Landlords
Task carried out in the public interest or in the exercise of official authority – Art 6(1)(e)	☒ Section 8 of the Data Protection Act 2018 Lawfulness of processing: public interest etc. In Article 6(1) of the UK GDPR (lawfulness of processing), the reference in point (e) to the processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority 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. Relevant authorities include Police, Probation providers, Health, Local Authorities and Registered Social Landlords. The Offender Management Act Section 14 Disclosure for Offender Management Purposes

	<i>NWP, HMPPS, BCUHB</i>
Legitimate Interest – Art 6(1)(f)	☒ Legitimate Interest will be the lawful basis for processing of personal data for the MARAC process for the third sector partner organisations, where they cannot rely on the Social Services & Wellbeing Wales Act 2014, and aren't classed as Competent Authorities Consideration is given by each partner organisation to the three part test:- ▪ The purpose test ▪ The necessity test ▪ The balancing test <i>3rd Sector Partner Organisations</i>

Table 2 - Article 9 - Special Categories of Personal Data

Legal basis	Checkbox / Notes
Necessary for reasons of substantial public interest - Art 9(2)(g)	☒ Section 10 of the Data Protection Act 2018 Special Categories of personal data and criminal convictions 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. 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: Condition 10 – preventing or detecting unlawful acts Condition 18 - safeguarding of children and of individuals at risk <i>All partners other than NWP, HMPPS, BCUHB and Local authority</i>
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)	☒ Section 10 of the Data Protection Act 2018 Special Categories of personal data and criminal convictions In Article 9(2) of the UK GDPR (Processing of special categories of data), the reference in point (h) that processing is necessary for the provision of health or social care <i>BCUHB and Local authority</i>

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	Processing is (select one): ☒ Carried out under the control of an official authority / competent authority NWP & HMPPS _____ and/or _____
	☒ Meets a relevant condition in Part 1, 2 or 3 of Schedule 1 of the Data Protection Act 2018. The relevant condition is: Schedule 1 Part 2 (10) preventing or detecting unlawful acts. All other partners

Table 4 - Competent authorities for Law Enforcement Purposes

Processing personal data for law enforcement purposes	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): ☐ 35(2)(a) The data subject has given consent. _____ or _____
	☒ 35(2)(b) The processing is necessary for the performance of a task carried out for that purpose by a competent authority. NWP and HMPPS
Sensitive processing / processing special categories of personal data for law enforcement purposes	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. The legal basis is (select one): ☐ 35(4) The data subject has given consent _____ or _____
	☒ 35(5) The processing is strictly necessary for the law enforcement purpose, and Meets a relevant condition in Schedule 8 of the Data Protection Act 2018. The relevant condition is: Condition 1 – statutory etc. purposes Condition 4 – safeguarding of children and individuals at risk NWP and HMPPS

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)	☒
Date of birth	☒
Address	☒
Postcode	☒
NHS Number	☒
PNCID	☒

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
- 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	Comments
	Website ☒		

North Wales Police	Leaflet ☐ Form ☐ Verbal ☒ Other (specify in comments) ☐	https://www.north-wales.police.uk/accessing-information-1/data-protection/privacy-notice-2018	The referring organisation will provide the data subject with privacy information verbally
BCUHB	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://bcuhb.nhs.wales/use-of-site/privacy-policy/	
Gwynedd Council	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	Council Services Privacy Notices (llyw.cymru)	
Youth Justice Service	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://www.gwynedd.llyw.cymru/en/Council/Information/Council-Services-Privacy-notices.aspx	
HMPPS	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	 HMPPS Privacy Notice.pdf	Privacy Notice displayed in each offender waiting area.
ADRA	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	Privacy - Adra	
BAWSO	Form ☐ Verbal ☐ Other (specify in comments) ☐	https://bawso.org.uk/assets/Uploads/BAWSO - Data protection Policy and Procedures	
ADFERIAD		Privacy Policy - Adferiad Recovery	
Grwp Cynefin		http://www.grwpcynefin.org/en/about-us/policies/	

North Wales Housing Association Gorwel		https://www.nwha.org.uk/about-us/data-protection/)	
		www.gorwel.org/eng/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 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 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.

9 Appendix A – Glossary of Terms

Term	Definition
Data Protection Act 2018	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. The 2018 Act also transposes EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law. It is important the UK 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 UK 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.
UK GDPR	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.
Law Enforcement Purposes	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)
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 data about criminal convictions, offences or related security measures	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))
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.' (UK GDPR Art 4(2))
Special categories of data / sensitive processing	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))
PNCID	This relates to the Police National Computer Identification number, allocated to an individual when entered on PNC.

10 **Appendix B – Information Reference Table for Gwynedd Multi Agency Risk Assessment Conference (MARAC)**

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	001 – Referral	002 – Assessment and Allocation to MARAC	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
1	Information exchange <i>General description of the process or stage to which the information sharing relates.</i>	Referral of potential MARAC case by any organisation/agency	Assessment undertaken by NWP Protecting Vulnerable Persons Unit by collecting further information from agencies other than the referring agency, and allocation of cases to be discussed at monthly MARAC	Discussion of cases at MARAC to identify risks posed to Service User, assess the needs of the Service User, agree and allocate the provision of appropriate services and review the provision of agreed services from previous meetings	NWP document minutes and actions from meeting and updates of intervention, and circulate to all partner organisations

2	What information will be shared? <i>Describe the information to be shared – you do not need to go to ‘field level’ detail.</i> <u>Please note: Only the minimum and relevant personal information is to be shared and strictly on a case by case basis.</u>	MARAC referrals may contain any or all of the following Personal identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal Identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal Identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status Details discussed at the MARAC meeting
---	--	--	---	---	---

3	Description	001 – Referral		002 – Assessment and Allocation to MARAC		003 – discussion at MARAC meeting and allocation of intervention		004 – distribution of minutes and actions	
		Who by	Who to	Who by	Who to	Who by	Who to	Who by	Who to
	Partner Organisation(s) <i>Details of provider and recipient organisation(s)</i> <i>Ensure the organisations listed reflect section 2 of the ISP i.e. are all organisations listed in section 2</i>	North Wales Police Betsi Cadwaladr UHB Gwynedd CC Youth Justice Service HMPPS ADRA BAWSO Adferiad Grwp Cynefin NW Housing Association Gorwel	North Wales Police	North Wales Police Betsi Cadwaladr UHB Gwynedd CC Youth Justice Service HMPPS ADRA BAWSO Adferiad Grwp Cynefin NW Housing Association Gorwel	North Wales Police	North Wales Police Betsi Cadwaladr UHB Gwynedd CC Youth Justice Service HMPPS ADRA BAWSO Adferiad Grwp Cynefin NW Housing Association Gorwel	North Wales Police Betsi Cadwaladr UHB Gwynedd CC Youth Justice Service HMPPS ADRA BAWSO Adferiad Grwp Cynefin NW Housing Association Gorwel	North Wales Police	North Wales Police Betsi Cadwaladr UHB Gwynedd CC Youth Justice Service HMPPS ADRA BAWSO Adferiad Grwp Cynefin NW Housing Association Gorwel

	Description	001 – Referral	002 – Assessment and Allocation to MARAC	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
4	How is information shared and what methods are used to keep the information secure? <i>Provide, in detail the specific agreed secure methods for sharing personal information</i>	Secure email, either using TLS1.2 or encrypted email	Secure email, either using TLS1.2 or encrypted email	Face to face meeting or secure online meeting (Microsoft Teams)	Minutes and actions sent out using Secure email, either using TLS1.2 or encrypted email
5	Reliance on consent <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>	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent

	Description	001 – Referral	002 – Assessment and Allocation to MARAC	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
6	Notes for Practitioners		Note: Although the schools are not partners to the MARAC process, they may be approached by the Education Welfare Officer to provide appropriate information as part of the research process prior to the MARAC.	Any printed documents or notes made during meeting must be securely destroyed	Note: Following each monthly MARAC meeting the MARAC Administrator forwards the minutes to all MARAC partners, along with an Action Tracker. These partners are then required to feedback on completed actions or those outstanding to the Public Protection Detective Sergeant, who will note them on subsequent minutes of the next MARAC meeting for discussion as appropriate. Following each weekly MARAC meeting, the MARAC administrator sends an Action Tracker to all partners, as above.

11 Appendix C – Partner Organisations Signatures

This section should only be completed once the ISP has been assured by a Quality Assurance group. Further information on the ISP development process can be found on the WASPI Website.

By signing below, partner organisations are confirming they agree with the content of the ISP. In the context of sharing personal information, signing the ISP is one way to demonstrate accountability with the principles set out in Article 5 of UK GDPR.

The signatory will be an appropriate person with authority to sign the ISP on behalf of the organisation. The ISP lead has responsibility for obtaining signatures to the ISP.

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	



Wales Accord on the Sharing of Personal Information

Information Sharing Protocol for

Multi Agency Risk Assessment Conference (MARAC) – Wrexham

Version V4.0 FINAL **Reviewed**

Date Assured December 2022

Quality Assurance Group North Wales QA Group

Contents

<i>1</i>	<i>Introduction to this ISP</i>	<i>2</i>
<i>2</i>	<i>The information sharing partner organisations</i>	<i>2</i>
<i>3</i>	<i>Specific organisational / practitioner obligations</i>	<i>3</i>
<i>4</i>	<i>Legislative / statutory powers</i>	<i>4</i>
<i>5</i>	<i>Personal information to be shared</i>	<i>8</i>
<i>6</i>	<i>Data Subjects' Rights</i>	<i>8</i>
<i>7</i>	<i>Information security</i>	<i>11</i>
<i>8</i>	<i>Review, Breaches and Termination of this Agreement</i>	<i>11</i>
<i>9</i>	<i>Appendix A – Glossary of Terms</i>	<i>12</i>
<i>10</i>	<i>Appendix B – Information Reference Table for Multi Agency Risk Assessment Conference (MARAC)</i>	<i>14</i>
<i>11</i>	<i>Appendix C – Partner Organisations Signatures</i>	<i>19</i>

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 dealing with high-risk cases of domestic abuse through the Multi Agency Risk Assessment Conference (MARAC) process in the Wrexham area.
- 1.4 Personal information is shared to enable appropriate actions to be taken to increase public safety. The responsibility to take appropriate actions rests with individual agencies; it is not transferred to the MARAC. Personal information is shared for the following purpose:
 - To increase the safety, health and well-being of victims and their children;
 - To determine whether the perpetrator poses a significant risk to any particular individual or to the general community;
 - To construct jointly and implement a risk management plan that provides professional support to all those at risk and that reduces the risk of harm;
 - To reduce repeat victimisation;
 - To improve agency accountability; and
 - To improve support for staff involved in high risk Domestic Abuse cases.

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
North Wales Police	Detective Inspector, Crime Services Protecting Vulnerable Persons Unit	Protecting Vulnerable Persons Unit
Betsi Cadwaladr University Health Board	Associate Director of Safeguarding Assistant Director of Nursing Assistant Area Director Childrens Central	Safeguarding Substance Misuse Service Mental Health Team CAMHS

Wrexham County Borough Council	Chief Officer Education and Early Intervention	Education Inclusion and ALN Education Social Work Education Prevention and Support - Youth Justice Service
	Chief Officer Housing & Economy	Housing
	Chief Officer Social Care	Children's Services Adult Social Care
HMPPS (Probation Service in Wales)	Head of North Wales Probation Delivery Unit	North Wales Probation Delivery Unit
BAWSO	Head of Regional Services	North Wales
Adferiad	Safeguarding Lead	Safeguarding Lead MARAC reps
Domestic Abuse Safety Unit (DASU)	Senior Manager, Wrexham and Flintshire	Wrexham and Flintshire DASU
	Senior Manager, Conwy and Denbighshire	Conwy and Denbighshire DASU
Relate Cymru (Choose to Change)	National Manager	Relate Cymru
Victim Support	Deputy Service Director	North Wales Victim Support (North Wales Victim Help Centre)
Wales and West Housing Association	Housing Manager	Housing
Grwp Cynefin Housing	Head of Communities	Housing

- 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
- 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
Necessary for compliance with a legal obligation – Art 6(1)(c)	☒ Social Services & Wellbeing (Wales) Act 2014 Part 7 – strengthens safeguarding responsibilities of organisations in relation to adults and children and the duty to report concerns. Part 9 requires local authorities to promote co-operation with relevant partners in relation to adults, children and carers and specifies arrangements for information sharing Local Authority, Registered Social Landlords
Task carried out in the public interest or in the exercise of official authority – Art 6(1)(e)	☒ Section 8 of the Data Protection Act 2018 Lawfulness of processing: public interest etc. In Article 6(1) of the UK GDPR (lawfulness of processing), the reference in point (e) to the processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority. 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. Relevant authorities include Police, Probation providers, Health, Local Authorities and Registered Social Landlords. The Offender Management Act Section 14 Disclosure for Offender Management Purposes <i>NWP, HMPPS, BCUHB</i>
Legitimate Interest – Art 6(1)(f)	☒ Legitimate Interest will be the lawful basis for processing of personal data for the MARAC process for the third sector partner organisations, where they cannot rely on the Social Services & Wellbeing Wales Act 2014, and aren't classed as Competent Authorities Consideration is given by each partner organisation to the three part test:- ▪ The purpose test ▪ The necessity test ▪ The balancing test <i>3rd Sector Partner Organisations</i>

Table 2 - Article 9 - Special Categories of Personal Data

Legal basis	Checkbox / Notes
Necessary for reasons of substantial public interest - Art 9(2)(g)	☒ Section 10 of the Data Protection Act 2018 Special Categories of personal data and criminal convictions 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. 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: Condition 10 – preventing or detecting unlawful acts Condition 18 - safeguarding of children and of individuals at risk <i>All partners other than NWP, HMPPS, BCUHB and Local authority</i>
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)	☒ Section 10 of the Data Protection Act 2018 Special Categories of personal data and criminal convictions In Article 9(2) of the UK GDPR (Processing of special categories of data), the reference in point (h) that processing is necessary for the provision of health or social care

	BCUHB and Local authority
--	----------------------------------

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	Processing is (select one): ☒ Carried out under the control of an official authority / competent authority Law Enforcement Agencies NWP & HMPPS _____ and/or _____
	☒ Meets a relevant condition in Part 1, 2 or 3 of Schedule 1 of the Data Protection Act 2018. The relevant condition is: Schedule 1 Part 2 (10) preventing or detecting unlawful acts. All other partners

Table 4 - Competent authorities for Law Enforcement Purposes

Processing personal data for law enforcement purposes	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): ☐ 35(2)(a) The data subject has given consent. _____ or _____
	☒ 35(2)(b) The processing is necessary for the performance of a task carried out for that purpose by a competent authority. NWP and HMPPS
Sensitive processing / processing special categories of personal data for law enforcement purposes	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. The legal basis is (select one): ☐ 35(4) The data subject has given consent _____ or _____
	☒ 35(5) The processing is strictly necessary for the law enforcement purpose, and Meets a relevant condition in Schedule 8.

	The relevant condition is: Condition 1 – statutory etc purposes Condition 4 – safeguarding of children and individuals at risk NWP and HMPPS
--	---

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)	☒
Date of birth	☒
Address	☒
Postcode	☒
NHS number	☒
PNCID	☒

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
- 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	Comments
North Wales Police	Website ☒ Leaflet ☐ Form ☐ Verbal ☒ Other (specify in comments) ☐	https://www.north-wales.police.uk/accessing-information-1/data-protection/privacy-notice-2018	The referring organisation will provide the data subject with privacy information verbally
BCUHB Wrexham CBC	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://bcuhb.nhs.wales/use-of-site/privacy-policy/ https://beta.wrexham.gov.uk/service/privacy-notice	
HMPPS (National Probation Service in Wales)	Website ☐ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☒	 HMPPS Privacy Notice.pdf	Privacy Notice displayed in each offender waiting area.
BAWSO Adferiad	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://bawso.org.uk/assets/Uploads/Bawso-Privacy-Policy.pdf Privacy Policy - Adferiad Recovery	
	Website ☒	https://www.dasunorthwales.co.uk/	

Domestic Abuse Safety Unit	Leaflet ☐ Form ☒ Verbal ☐ Other (specify in comments) ☐		
Relate Cymru	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	https://www.relate.org.uk/cymru/privacy	
Victim Support	Website ☒ Leaflet ☒ Form ☐ Verbal ☒ Other (specify in comments) ☐	 Full Service Delivery Fair Processing Notice	Privacy information provided using website, letter and also verbal.
Wales and West Housing	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☒	https://www.wwha.co.uk/en/legal/	
Grwp Cynefin Housing	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other (specify in comments) ☐	Privacy GDPR - Grŵp Cynefin (grwpcynefin.org)	

- 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 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 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
Data Protection Act 2018	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. The 2018 Act also transposes EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law. It is important the UK 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 UK 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.
UK GDPR	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.
Law Enforcement Purposes	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)
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 data about criminal convictions, offences or related security measures	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))
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.' (UK GDPR Art 4(2))
Special categories of data / sensitive processing	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))
PNCID	This relates to the Police National Computer Identification number, allocated to an individual when entered on PNC.

10 **Appendix B – Information Reference Table for Multi Agency Risk Assessment Conference (MARAC)**

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	001 – Referral	002 – Assessment and Allocation	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
1	Information exchange <i>General description of the process or stage to which the information sharing relates.</i>	Referral of potential MARAC case by any organisation/agency	Assessment undertaken by NWP Protecting Vulnerable Persons Unit by collecting further information from agencies other than the referring agency, and allocation of cases to be discussed at monthly MARAC	Discussion of cases at MARAC to identify risks posed to Service User, assess the needs of the Service User, agree and allocate the provision of appropriate services and review the provision of agreed services from previous meetings	NWP document minutes and actions from meeting and updates of intervention, and circulate to all partner organisations

2	What information will be shared? <i>Describe the information to be shared – you do not need to go to ‘field level’ detail.</i> <u>Please note: Only the minimum and relevant personal information is to be shared and strictly on a case by case basis.</u>	MARAC referrals may contain any or all of the following Personal identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal Identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal Identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status Details discussed at the MARAC meeting
---	--	--	---	---	---

3	Description	001 – Referral		002 – Assessment and Allocation		003 – discussion at MARAC meeting and allocation of intervention		004 – distribution of minutes and actions	
		Who by	Who to	Who by	Who to	Who by	Who to	Who by	Who to
	Partner Organisation(s) <i>Details of provider and recipient organisation(s)</i> <i>Ensure the organisations listed reflect section 2 of the ISP i.e. are all organisations listed in section 2</i>	North Wales Police Betsi Cadwaladr UHB Wrexham CBC HMPPS BAWSO Adferiad Domestic Abuse Safety Unit Relate Cymru Victim Support Wales and West Housing Grwp Cynefin Housing	North Wales Police	North Wales Police Betsi Cadwaladr UHB Wrexham CBC HMPPS BAWSO Adferiad Domestic Abuse Safety Unit Relate Cymru Victim Support Wales and West Housing Grwp Cynefin Housing	North Wales Police	North Wales Police Betsi Cadwaladr UHB Wrexham CBC HMPPS BAWSO Adferiad Domestic Abuse Safety Unit Relate Cymru Victim Support Wales and West Housing Grwp Cynefin Housing	North Wales Police Betsi Cadwaladr UHB Wrexham CBC HMPPS BAWSO Adferiad Domestic Abuse Safety Unit Relate Cymru Victim Support Wales and West Housing Grwp Cynefin Housing	North Wales Police	North Wales Police Betsi Cadwaladr UHB Wrexham CBC HMPPS BAWSO Adferiad Domestic Abuse Safety Unit Relate Cymru Victim Support Wales and West Housing Grwp Cynefin Housing

	Description	001 – Referral	002 – Assessment and Allocation	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
4	How is information shared and what methods are used to keep the information secure? <i>Provide, in detail the specific agreed secure methods for sharing personal information</i>	Secure email, either using TLS1.2 or encrypted email	Secure email, either using TLS1.2 or encrypted email	Face to face meeting or secure online meeting (Microsoft Teams)	Minutes and actions sent out using Secure email, either using TLS1.2 or encrypted email
5	Reliance on consent <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>	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent

	Description	001 – Referral	002 – Assessment and Allocation	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
6	Notes for Practitioners		Note: Although the schools are not partners to the MARAC process, they may be approached by the Education Welfare Officer to provide appropriate information as part of the research process prior to the MARAC.	Any printed documents or notes made during meeting must be securely destroyed	Note: Following each monthly MARAC meeting the MARAC Administrator forwards the minutes to all MARAC partners, along with an Action Tracker. These partners are then required to feedback on completed actions or those outstanding to the Public Protection Detective Sergeant, who will note them on subsequent minutes of the next MARAC meeting for discussion as appropriate. Following each weekly MARAC meeting, the MARAC administrator sends an Action Tracker to all partners, as above.

11 **Appendix C – Partner Organisations Signatures**

This section should only be completed once the ISP has been assured by a Quality Assurance group. Further information on the ISP development process can be found on the WASPI Website.

By signing below, partner organisations are confirming they agree with the content of the ISP. In the context of sharing personal information, signing the ISP is one way to demonstrate accountability with the principles set out in Article 5 of UK GDPR.

The signatory will be an appropriate person with authority to sign the ISP on behalf of the organisation. The ISP lead has responsibility for obtaining signatures to the ISP.

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation	Wrexham County Borough Council	Partner Organisation	
Name	Ian Bancroft	Name	
Position	Chief Executive Officer	Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	



Wales Accord on the Sharing of Personal Information

Information Sharing Protocol for Multi Agency Risk Assessment Conference (MARAC) – Ynys Mon

Version **Reviewed** V4.0 FINAL

Date Assured December 2022

Quality Assurance Group North Wales QA Group

Contents

<i>1</i>	<i>Introduction to this ISP</i>	<i>3</i>
<i>2</i>	<i>The information sharing partner organisations</i>	<i>3</i>
<i>3</i>	<i>Specific organisational / practitioner obligations</i>	<i>4</i>
<i>4</i>	<i>Legislative / statutory powers</i>	<i>5</i>
<i>5</i>	<i>Personal information to be shared</i>	<i>8</i>
<i>6</i>	<i>Data Subjects' Rights</i>	<i>9</i>
<i>7</i>	<i>Information security</i>	<i>11</i>
<i>8</i>	<i>Review, Breaches and Termination of this Agreement</i>	<i>11</i>
<i>9</i>	<i>Appendix A – Glossary of Terms</i>	<i>12</i>
<i>10</i>	<i>Appendix B – Information Reference Table for Ynys Mon Multi Agency Risk Assessment Conference (MARAC)</i>	<i>14</i>
<i>11</i>	<i>Appendix C – Partner Organisations Signatures</i>	<i>19</i>

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 dealing with high-risk cases of domestic abuse through the Multi Agency Risk Assessment Conference (MARAC) process in the Ynys Mon area.
- 1.4 Personal information is shared to enable appropriate actions to be taken to increase public safety. The responsibility to take appropriate actions rests with individual agencies; it is not transferred to the MARAC. Personal information is shared for the following purpose:
 - To increase the safety, health and well-being of victims and their children;
 - To determine whether the perpetrator poses a significant risk to any particular individual or to the general community;
 - To construct jointly and implement a risk management plan that provides professional support to all those at risk and that reduces the risk of harm;
 - To reduce repeat victimisation;
 - To improve agency accountability; and
 - To improve support for staff involved in high risk Domestic Abuse cases.

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
North Wales Police	Detective Inspector, Crime Services Protecting Vulnerable Persons Unit	Protecting Vulnerable Persons Unit
Betsi Cadwaladr University Health Board	Associate Director of Safeguarding Assistant Director of Nursing Assistant Area Director Childrens Central	Safeguarding Substance Misuse Service Mental Health Team CAMHS
Cyngor Sir Ynys Mon	Director of Education, skills and Young People	Education

	Head of Children and Families Services	Children's Services
	Head of Adult Services	Adult Services
	Head of Housing Services	Housing
Youth Justice Service (Gwynedd ac Ynys Mon)	Service Manager	Youth Justice Service
HMPPS (Probation Service in Wales)	Head of North Wales Probation Delivery Unit	North Wales Probation Delivery Unit
BAWSO	Head of Regional Services	North Wales
ADFERIAD	Service Manager	ADFERIAD
ADRA	Neighbourhood Services Assistant Manager (North)	Housing
Grwp Cynefin	Head of Communities	Operations
North Wales Housing Association	Director of Operations	North Wales Housing
Gorwel	IDVA Team Leader/Safeguarding	IDVA Team

- 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
- 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
Necessary for compliance with a legal obligation – Art 6(1)(c)	☒ Social Services & Wellbeing (Wales) Act 2014 Part 7 – strengthens safeguarding responsibilities of organisations in relation to adults and children and the duty to report concerns. Part 9 requires local authorities to promote co-operation with relevant partners in relation to adults, children and carers and specifies arrangements for information sharing Local Authority, Registered Social Landlords
Task carried out in the public interest or in the exercise of official authority – Art 6(1)(e)	☒ Section 8 of the Data Protection Act 2018 Lawfulness of processing: public interest etc. In Article 6(1) of the UK GDPR (lawfulness of processing), the reference in point (e) to the processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority 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. Relevant authorities include Police, Probation providers, Health, Local Authorities and Registered Social

	Landlords. The Offender Management Act Section 14 Disclosure for Offender Management Purposes <i>NWP, HMPPS, BCUHB</i>
Legitimate Interest – Art 6(1)(f)	☒ Legitimate Interest will be the lawful basis for processing of personal data for the MARAC process for the third sector partner organisations, where they cannot rely on the Social Services & Wellbeing Wales Act 2014, and aren't classed as Competent Authorities Consideration is given by each partner organisation to the three part test:- ▪ The purpose test ▪ The necessity test ▪ The balancing test <i>3rd Sector Partner Organisations</i>

Table 2 - Article 9 - Special Categories of Personal Data

Legal basis	Checkbox / Notes
Necessary for reasons of substantial public interest - Art 9(2)(g)	☒ Section 10 of the Data Protection Act 2018 Special Categories of personal data and criminal convictions Art 9(2)(g) requires a basis in UK law, which is provided by UK GDPR Section 10(3) of the Data Protection Act 2018. 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: Condition 10 – preventing or detecting unlawful acts Condition 18 - safeguarding of children and of individuals at risk <i>All partners other than NWP, HMPPS, BCUHB and Local authority</i>
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)	☒ Section 10 of the Data Protection Act 2018 Special Categories of personal data and criminal convictions In Article 9(2) of the UK GDPR (Processing of special categories of data), the reference in point (h) that processing is necessary for the provision of health or social care <i>BCUHB and Local authority</i>

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	Processing is (select one): ☒ Carried out under the control of an official authority / competent authority Law Enforcement Agencies NWP & HMPPS _____ and/or _____
	☒ Meets a relevant condition in Part 1, 2 or 3 of Schedule 1 of the Data Protection Act 2018. The relevant condition is: Schedule 1 Part 2 (10) preventing or detecting unlawful acts. All other partners

Table 4 - Competent authorities for Law Enforcement Purposes

Processing personal data for law enforcement purposes	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): ☐ 35(2)(a) The data subject has given consent. _____ or _____
	☒ 35(2)(b) The processing is necessary for the performance of a task carried out for that purpose by a competent authority. NWP and HMPPS
Sensitive processing / processing special categories of personal data for law enforcement purposes	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. The legal basis is (select one): ☐ 35(4) The data subject has given consent _____ or _____
	☒ 35(5) The processing is strictly necessary for the law enforcement purpose, and Meets a relevant condition in Schedule 8 of the Data Protection Act 2018. The relevant condition is: Condition 1 – statutory etc. purposes Condition 4 – safeguarding of children and individuals at risk NWP and HMPPS

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)	☒
Date of birth	☒
Address	☒
Postcode	☒
NHS number	☒
PNCID	☒

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
- 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	Name of document / website	Con
----------------------	--	---------------------	----------------------------	-----

		(select any that apply)		
North Wales Police	Website	☒	https://www.north-wales.police.uk/accessing-information-1/data-protection/privacy-notice-2018	The refer orga will p the c subje privat infor verbo
	Leaflet	☐		
	Form	☐		
	Verbal	☒		
	Other (specify in comments)	☐		
BCUHB	Website	☒	https://bcuhb.nhs.wales/use-of-site/privacy-policy/	
	Leaflet	☐		
	Form	☐		
	Verbal	☐		
	Other (specify in comments)	☐		
Cyngor Sir Ynys Mon	Website	☒	https://www.anglesey.gov.uk/en/Residents/Adult-social-care/Privacy-Notice-Adult-Social-Care.aspx	
	Leaflet	☐		
	Form	☐		
	Verbal	☐		
	Other (specify in comments)	☐		
Youth Justice Service	Website	☒	https://www.gwynedd.llyw.cymru/en/Council/Information/Council-Services-Privacy-notice.aspx	
	Leaflet	☐		
	Form	☐		
	Verbal	☐		
	Other (specify in comments)	☐		
HMPPS (National Probation Service in Wales)	Website	☐		Priva Notic displ each offer waiti
	Leaflet	☐	HMPPS Privacy Notice.pdf	
	Form	☐		
	Verbal	☐		
	Other (specify in comments)	☒		
BAWSO	Website	☒	https://bawso.org.uk/assets/Uploads/Bawso-Privacy-Policy.pdf	
Adferiad	Leaflet	☐	Privacy Policy - Adferiad Recovery	
ADRA	Form	☐	Privacy - Adra	
	Verbal	☐		

Grwp Cynefin	Other (specify in comments)	☐	http://www.grwpcynefin.org/en/about-us/policies/
North Wales Housing Association			https://www.nwha.org.uk/about-us/data-protection/)
Gorwel			www.gorwel.org/eng/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 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 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.

9 Appendix A – Glossary of Terms

Term	Definition
Data Protection Act 2018	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. The 2018 Act also transposes EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law. It is important the UK 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 UK 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.
UK GDPR	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.
Law Enforcement Purposes	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)
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 data about criminal convictions, offences or related security measures	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))
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.' (UK GDPR Art 4(2))
Special categories of data / sensitive processing	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))
PNCID	This relates to the Police National Computer Identification number, allocated to an individual when entered on PNC.

10 **Appendix B – Information Reference Table for Ynys Mon Multi Agency Risk Assessment Conference (MARAC)**

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	001 – Referral	002 – Assessment and Allocation to MARAC	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
1	Information exchange <i>General description of the process or stage to which the information sharing relates.</i>	Referral of potential MARAC case by any organisation/agency	Assessment undertaken by NWP Protecting Vulnerable Persons Unit by collecting further information from agencies other than the referring agency, and allocation of cases to be discussed at monthly MARAC	Discussion of cases at MARAC to identify risks posed to Service User, assess the needs of the Service User, agree and allocate the provision of appropriate services and review the provision of agreed services from previous meetings	NWP document minutes and actions from meeting and updates of intervention, and circulate to all partner organisations

2	What information will be shared? <i>Describe the information to be shared – you do not need to go to ‘field level’ detail.</i> <u>Please note: Only the minimum and relevant personal information is to be shared and strictly on a case by case basis.</u>	MARAC referrals may contain any or all of the following Personal identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal Identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal Identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status	Personal identifiers Health / wellbeing information Offending history Risks / safeguarding issues Family / personal history / personal profile Family status •Marital / relationship status •No. of dependents Housing status Details discussed at the MARAC meeting
---	--	--	---	---	---

3	Description	001 – Referral		002 – Assessment and Allocation to MARAC		003 – discussion at MARAC meeting and allocation of intervention		004 – distribution of minutes and actions	
		Who by	Who to	Who by	Who to	Who by	Who to	Who by	Who to
	Partner Organisation(s) <i>Details of provider and recipient organisation(s)</i> <i>Ensure the organisations listed reflect section 2 of the ISP i.e. are all organisations listed in section 2</i>	North Wales Police Betsi Cadwaladr UHB Gwynedd CC Youth Justice Service HMPPS BAWSO Adferiad ADRA Grwp Cynefin NW Housing Association Gorwel	North Wales Police	North Wales Police Betsi Cadwaladr UHB Gwynedd CC Youth Justice Service HMPPS BAWSO Adferiad ADRA Grwp Cynefin NW Housing Association Gorwel	North Wales Police	North Wales Police Betsi Cadwaladr UHB Gwynedd CC Youth Justice Service HMPPS BAWSO Adferiad ADRA Grwp Cynefin NW Housing Association Gorwel	North Wales Police Betsi Cadwaladr UHB Gwynedd CC Youth Justice Service HMPPS BAWSO Adferiad ADRA Grwp Cynefin NW Housing Association Gorwel	North Wales Police	North Wales Police Betsi Cadwaladr UHB Gwynedd CC Youth Justice Service HMPPS BAWSO Adferiad ADRA Grwp Cynefin NW Housing Association Gorwel

	Description	001 – Referral	002 – Assessment and Allocation to MARAC	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
4	How is information shared and what methods are used to keep the information secure? <i>Provide, in detail the specific agreed secure methods for sharing personal information</i>	Secure email, either using TLS1.2 or encrypted email	Secure email, either using TLS1.2 or encrypted email	Face to face meeting or secure online meeting (Microsoft Teams)	Minutes and actions sent out using Secure email, either using TLS1.2 or encrypted email
5	Reliance on consent <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>	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ Exchange relies on consent ☒ Exchange does not rely on consent

	Description	001 – Referral	002 – Assessment and Allocation to MARAC	003 – discussion at MARAC meeting and allocation of intervention	004 – distribution of minutes and actions
6	Notes for Practitioners		Note: Although the schools are not partners to the MARAC process, they may be approached by the Education Welfare Officer to provide appropriate information as part of the research process prior to the MARAC.	Any printed documents or notes made during meeting must be securely destroyed	Note: Following each monthly MARAC meeting the MARAC Administrator forwards the minutes to all MARAC partners, along with an Action Tracker. These partners are then required to feedback on completed actions or those outstanding to the Public Protection Detective Sergeant, who will note them on subsequent minutes of the next MARAC meeting for discussion as appropriate. Following each weekly MARAC meeting, the MARAC administrator sends an Action Tracker to all partners, as above.

11 Appendix C – Partner Organisations Signatures

This section should only be completed once the ISP has been assured by a Quality Assurance group. Further information on the ISP development process can be found on the WASPI Website.

By signing below, partner organisations are confirming they agree with the content of the ISP. In the context of sharing personal information, signing the ISP is one way to demonstrate accountability with the principles set out in Article 5 of UK GDPR.

The signatory will be an appropriate person with authority to sign the ISP on behalf of the organisation. The ISP lead has responsibility for obtaining signatures to the ISP.

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	

Partner Organisation		Partner Organisation	
Name		Name	
Position		Position	
Date		Date	
Signature		Signature	