Wales Accord on the Sharing of Personal Information

Information Sharing Protocol for Cwm Taf Prevent and Channel Programme

Version: v1.0

Contents

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 between the participating partner organisations. Partners have given consideration to its contents when drawing up this document.

1.2 This ISP has been prepared to support the regular sharing of personal information for the discharge of the Prevent and Channel duties in the Cwm Taf area in line with those described in the Counter Terrorism and Security Act 2015.

1.3 Channel is part of the Prevent Strategy. The process is a multi-agency approach to identify and provide support to individuals who are at risk of being drawn into terrorism. The programme uses a multi-agency approach to protect vulnerable people by identifying individuals at risk, assessing the nature and extent of the risk, developing the most appropriate support plan for the individuals concerned.

1.4 This ISP covers the exchange of information between local authorities, the Police Force and Health Board.

1.5 It supports the information sharing partner organisations involved and the groups of service users it impacts upon. It details the specific purposes for sharing and the personal information being shared, the required operational procedures, consent processes, and legal justification.

1.6 This ISP should be read in conjunction with the Channel Guidance published on the .gov.uk website.

1.7 For the purpose of this ISP, **explicit consent** is required from service users.

1.8 Partners may only use the information disclosed to them under this ISP for the specific purpose(s) set out in this document or to support the effective administration, audit, monitoring, inspection of services and reporting requirements.

1.9 A glossary of terms for this ISP is contained within Appendix A.

Please note: 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.

2 The information sharing partner organisations

2.1 This ISP covers the exchange of information between practitioners of the following organisations:

Information Sharing Partner Organisations	Responsible Manager
1. Merthyr Tydfil County Borough Council (MTCBC)	Housing & Community Safety Manager
2. Rhondda Cynon Taf County Borough Council (RCTCBC)	Community & Safety Licencing Manager
3. South Wales Police (SWP)	Channel Coordinator

4. Cwm Taf Health Board (CTHB)	Head of Safeguarding
5. National Probation Service (NPS)	Team Manager
6. Merthyr Valley Homes (MVH)	Head of Housing
7. Merthyr Tydfil Housing Association (MTHA)	Housing Services Manager
8. Trivallis Housing Association (TVA)	Tenancy Management Officer
9. Newydd Housing (NH)	Anti-Social Behaviour Coordinator
10. Wales Ambulance Service NHS Trust (WAST)	Safeguarding Lead Officer
11. The College Merthyr Tydfil (TCMT)	Learner Welfare Services Officer
12. University of South Wales (USW)	Director of Chaplaincy Services
13. Cwm Taf Youth Offending Service (CTYOS)	Operational Manager
14. Wales Community Rehabilitation Company (WCRC)	Team Manager
15. Coleg Y Cymoedd (CYC)	Director of Learner Services

2.2 The responsible managers detailed above have overall responsibility for this ISP within their own organisations, and must therefore ensure the ISP is disseminated, understood and acted upon by relevant practitioners.

2.3 The responsible manager from each partner organisation will regularly monitor and audit access to information shared under this ISP to ensure appropriate access is maintained.

3 Benefits of sharing

3.1 By sharing personal information under this ISP, it is envisaged that the following benefits will be achieved:

- Identify individuals and networks that are turning to violent or non-violent extremism or who are vulnerable people being radicalised and drawn into terrorism;
- Enable measures to be developed aimed at facilitating the delivery of effective interventions and so divert vulnerable persons from turning to violent or non-violent extreme behaviour.

4 Legislative / statutory powers

4.1 Disclosure of information will be conducted within the legal framework of the Data Protection Act 1998 (DPA), the Human Rights Act 1998 and in compliance with the common law duty of confidence.

4.2 The conditions set out in Schedule 2 and 3 of the DPA are known as the “conditions for processing”. Organisations processing personal data need to be able to satisfy one or more of these conditions. For the purpose of this ISP, the condition that will be relied upon for both Schedules (where required) is **explicit consent**. Therefore no further conditions need to be met.

4.3 In addition to relying on consent as a Schedule condition, public bodies may have statutory requirements to share some types of personal data. In the absence of a statutory requirement, a public sector body should be able to explain the legal power it has to enable it to share. Other organisations may not need statutory powers to share.

4.4 Additional provisions of power provided to partner organisations undertaking statutory duties in the sharing of information are:

- Counter Terrorism and Security Act 2015
- Social Services and Well-being (Wales) Act 2014
- Channel Duty Guidance, Protecting Vulnerable People from being drawn into Terrorism, Statutory Guidance for Channel Panel Members and Partners of Local Panels
- The Data Protection Act 1998, sections 29(3) & 35(2)
- Data Protection (Processing of Sensitive Personal Data) Order 2000
- The Human Rights Act 1998, article 8
- Common Law Duty of Confidentiality
- The Crime and Disorder Act 1998, section 115
- Common Law Powers
- Local Government Act 2000, section 2(1)
- National Health Service Act (NHSA) 2006, section 251, and Health and Social Care Act (HCSA) 2001, section 60
- Offender Management Act 2007, section 14

5 Details of personal information being shared

5.1 Personal information shared for the purpose of this ISP includes a range of information and might therefore include:

- Alias
- Forename(s)
- Surname
- Address/Housing Circumstances
- Gender
- DOB
- Ethnicity
- Current Employment Status
- Medical History
- Criminal Records
- Religious Beliefs
- Reason for Referral (full details of vulnerabilities and/or causes)
- History of Violence

5.2 The information is used to refer individuals and for the Channel Panel to discuss what support and actions may be taken to safeguard the referral where vulnerabilities have been identified. The Channel Programme is about individuals receiving support and

intervention before their vulnerabilities are exploited by those that would want them to terrorism and before they become involved in criminal terrorist activity.

5.3 Only the **minimum necessary** personal information consistent with the purposes set out in this document can be shared.

5.4 Information provided by partner organisations will not generally be released to any third party without prior consultation with the owning partner organisation.

5.5 An information reference table within Appendix B provides a comprehensive list of the personal information to be shared between the partner organisations, including with whom in each partner organisation it will be shared with, why it will be shared and the methods of how it will be shared.

6 Identifying the service user

6.1 In order to ensure that all partner organisations, when sharing information, are referring to the same service user, the following personal identifiers must be included:

- Alias
- Forename(s)
- Surname
- Address
- DOB

7 Informing the service user

7.1 It is necessary to communicate with the service user or their lawful representatives about the need for information sharing at the earliest appropriate opportunity, preferably at first contact unless by doing so would risk harm to others or hinder any investigation or legal proceedings.

7.2 Therefore in most cases practitioners will clearly inform service users or their lawful representatives about what personal information is to be shared, and for what purposes it will be used. Partner organisations should also ensure that service users are provided with any information they need to fully understand the way in which their personal data will be handled in any specific circumstance, including the names of any persons or organisations with whom their data may be shared.

7.3 Where appropriate, agreed methods of providing this information are:

- At the earliest opportunity, Practitioners will clearly inform service users or their lawful representatives about what personal information is to be shared, and for what purposes it will be used;
- The Channel Guidance document provides information on the consent requirements and how the subject's information will be processed.

8 Obtaining consent

8.1 The approach to obtaining consent should be transparent and respect the rights of the service user.

8.2 Consent is given by a service user agreeing actively, to a particular use or disclosure of information. It can be expressed either verbally or in writing, although written consent is preferable since that reduces the scope for subsequent dispute. For the purposes of this ISP, **explicit consent** will be required from service users.

8.3 Consent must not be secured through coercion or inferred from a lack of response to a request for consent. Practitioners must be satisfied that the service user has understood the information sharing arrangements and the consequences of providing or withholding consent.

8.4 Where a service user is a child or young person, the practitioner should consider whether the child or young person has the capacity to understand the implications of giving their consent in the particular circumstance. Where the practitioner is confident that the child or young person can understand their rights, then consent should be sought from them rather than a parent. It is important that a child or young person is able to understand (in broad terms) what it means to give their consent.

8.5 Consent should not be regarded as a permanent state. Opportunities to review the service user's continuing consent to information sharing should arise during the course of the service provision. Practitioners should exercise professional judgement in determining whether it would be appropriate to re-visit a service user's continued consent at any given juncture. Ideally it should take place in the context of a review or re-assessment.

8.6 Consent obtained from service users for the purposes of this ISP will only be used to support the delivery of the purposes and functions set out in this document. Once the provision of this specific ISP concludes or the purpose changes, then consent obtained for it will also end.

8.7 In some exceptional circumstances, personal information can be lawfully shared without consent where there is a legal requirement or where an appropriate professional of sufficient seniority within the partner organisation, has taken the view that the duty of confidentiality can be breached where there is a substantial over-riding 'public interest'. Such situations where information might be shared without consent include:

- 'Life and death' situations, for example, where information is shared in an emergency in order to preserve life;
- where a person's condition indicates they may be a risk to the public or may inflict self-harm;
- in order to prevent abuse or serious harm to others;
- on a case-by-case basis, to prevent serious crime and support detection, investigation and punishment of serious crime.

This is not an exhaustive list and each situation should be considered on a case by case basis.

8.8 Where decisions are made to share personal information without the service user's consent, as detailed above in 8.7, this must be fully documented in the service user's record.

8.9 Where it is not appropriate to defer the sharing of information, then it will not be appropriate to defer consent, as consent cannot be obtained retrospectively. Therefore, only where deemed necessary, may information be shared without consent.

8.10 If there are any concerns relating to child or adult protection issues, practitioners must follow the relevant organisational procedures.

9 Obtaining consent where a service user lacks mental capacity

9.1 The Mental Capacity Act 2005 Code of Practice defines the term 'a person who lacks capacity' as a person who lacks capacity to make a particular decision or take a particular action for themselves, at the time the decision or action needs to be taken.

9.2 Whenever dealing with issues of capacity to consent, local rules and procedures should be followed and these must be in compliance with the Mental Capacity Act 2005 and its Code of Practice.

9.3 Where a person has a temporary loss of capacity consent will be deferred, if appropriate, until such time as consent can be obtained. Consent to share information will be sought when capacity is regained.

10 Recording consent

10.1 Decisions regarding service users' consent of how and when it was obtained and whether it was provided in verbal or in written form, must be stored or recorded in the service user's record.

11 Refused and withdrawn consent

11.1 A service user has the right to refuse their consent to have information about them shared. They also have the right to withdraw previously granted consent at any point, to the sharing of their information. Further personal information should not then be shared under this ISP.

11.2 Where the service user has refused or withdrawn consent, the implications of withholding consent will be clearly explained to them and this dialogue will be recorded in the service user's record. If a service user withdraws consent to share personal information it will also be explained that information already shared cannot be recalled.

12 Information security

12.1 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.

12.2 Where practitioners are unable to comply with their organisation's policies regarding the safe and secure transfer of information they must ensure that a risk assessment is undertaken by their Information Security/Governance department at the earliest opportunity. Alternative secure methods, as identified within the organisation's policy, must be used until such time as the risk assessment has been undertaken.

12.3 A list of agreed methods for the safe and secure transfer of personal information is documented within Appendix B.

12.4 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 share, where appropriate, the outcome of any investigation with the partner organisations involved.

13 Records management

13.1 Practitioners carrying out the functions outlined in this ISP should make themselves aware of, and adhere to, their organisation's records management procedures, specifically in relation to collecting, processing and disclosing of personal information.

13.2 All information, whether held on paper or in electronic format must be stored and disposed of in line with each partner organisation's retention and disposal schedule.

13.3 Personal information will only be collected using the agreed collection methods, ensuring the required information is complete and up-to-date.

13.4 Practitioners will ensure where practical, that records are maintained of when information is shared with a partner organisation, and to whom.

13.5 Decisions about service users should never be made by referring to inaccurate, incomplete or out of date information.

13.6 If information is found to be inaccurate, practitioners will ensure that their records and systems are corrected accordingly. Consideration must also be given to advising partner organisations where practical.

14 Data Protection Act and Freedom of Information Act requests

14.1 Where requests are received for information relating to this ISP or any individual service user(s) then each request will be dealt with in accordance with each partner organisation's relevant policies and procedures.

15 Complaints

15.1 Each partner organisation has a formal procedure by which service users, partner organisations and practitioners can direct, their complaints regarding the application of this ISP.

16 Review of this ISP

16.1 This ISP will be reviewed after one year and then every two years thereafter, or sooner if appropriate. Merthyr Tydfil County Borough Council (MTCBC) will be the lead authority for the review.

17 Appendix A – Glossary of Terms

Term	Definition
Consent	An informed indication by which the service user signifies agreement and understanding of how personal information relating to them is processed.
Personal information	Information which relates to an individual, including their image or voice, which enables them to be uniquely identified from that information on its own or from that and / or other information available to that organisation. It includes personal data within the meaning of Section 1 of the Data Protection Act 1998 and information relating to the deceased.
Sensitive personal information	Personal information as to; the racial or ethnic origin of an individual; their political opinions, their religious beliefs or other beliefs of a similar nature, whether they are a member of a trade union, their physical or mental health or condition, their sexual life, the commission or alleged commission by them of any offence, or any proceedings for an offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.
Personal identifiers	A set of basic personal details that allow partner organisations to identify exactly who is being referred to. For example, name, address, date of birth, post code.
Processing personal information	Broadly describes the collecting, using, disclosing, retaining or disposing, of personal information. If any aspects of processing are found to be unfair, then the Data Protection Act 1998 is likely to be breached.
Service user	An inclusive term to describe those people who have contact with service providing organisations within Wales and have information recorded about them. For example: individual organisations may refer to these people as data subjects, patients, clients, lawful representatives, etc.
Practitioner	An inclusive term to describe any staff working for the partner organisations involved in the care of or provision of services for the service user. For example: police officer, health professional, social worker, volunteer etc.
Responsible Manager	A senior manager within an organisation who has overall responsibility for the area of work related to a specific ISP. It will be their responsibility to ensure that ISPs are disseminated, understood and acted upon by relevant practitioners and that access to personal information is regularly monitored and audited to ensure appropriate access is maintained.

18 Appendix B – Information Reference Table

The sharing of personal information to support the provision of Cwm Taf Prevent and Channel Programme				
	Description	**Identification and referral of concern / Preliminary Assessment**	**Channel Panel Meeting**	**Channel Intervention**
1	**Information exchange** General description of the process or stage to which the information exchange relates.	Agency/partner makes referral detailing full vulnerability and causes, why the subject is suitable for Prevent intervention, if radicalised, also if the individual has difficulties integrating into society. The Police Channel Panel Coordinator gathers additional information to ensure referral is genuine, not malicious, misguided or misinformed.	If case is deemed appropriate for Channel, it is brought to quarterly Channel meeting to discuss and assess risks, support needs and whether specialist intervention is required.	Channel intervention will be commissioned from an approved provider. People deemed appropriate to receive support will have a tailored package developed for them, according to their identified vulnerabilities. The provider used for each case depends on the individual and their needs, as well as the type of the case/intervention which is agreed by the group.
2	**What information will be shared?** Description of the information to be provided. **Please note**: Only the minimum and relevant personal information is to be shared and strictly on a case by case basis.	Demographic information; Medical information; Criminal information; Family information; As per section 5.	Demographic information; Medical information; Criminal information; Family information; As per section 5; Support needs, if any.	Demographic information; Medical information; Criminal information; Family information; As per section 5; Support needs, if any.
3	**Consent to share** Details of when and how consent will be sought.	Practitioners will clearly inform service users or their legal representatives, what information will be shared and who it will be shared with.	The Channel Chair is responsible for ensuring an effective support plan is put in place, and that consent is sought from the individual before that plan is put in place.	As participation in Channel remains voluntary, section 36(4)(b) of the CT&S Act requires consent to be given by the individual (or their parent/guardian in case of a child) in advance of support measures being put in place. Where someone does not wish to continue with the process, it

				may be appropriate to provide alternative support through other mainstream services, such as Children or Adult Social Care Services.

	Description	Identification and referral of concern / Preliminary Assessment		Channel Panel Meeting		Channel Intervention	
4	**Partner Organisation(s)**	**Who by**	**Who to**	**Who by**	**Who to**	**Who by**	**Who to**
a	Details of provider and recipient organisation(s).	1. MTCBC 2. RCTCBC 3. SWP 4. CTHB 5. NPS 6. MVH 7. MTHA 8. TVA 9. NH 10. WAST 11. TCMT 12. USW 13. CTYOS 14. WCRC 15. CYC	3. SWP	1. MTCBC 2. RCTCBC 3. SWP 4. CTHB 5. NPS 6. MVH 7. MTHA 8. TVA 9. NH 10. WAST 11. TCMT 12. USW 13. CTYOS 14. WCRC 15. CYC	1. MTCBC 2. RCTCBC 3. SWP 4. CTHB 5. NPS 6. MVH 7. MTHA 8. TVA 9. NH 10. WAST 11. TCMT 12. USW 13. CTYOS 14. WCRC 15. CYC	1. MTCBC 2. RCTCBC 3. SWP 4. CTHB 5. NPS 6. MVH 7. MTHA 8. TVA 9. NH 10. WAST 11. TCMT 12. USW 13. CTYOS 14. WCRC 15. CYC	1. MTCBC 2. RCTCBC 3. SWP 4. CTHB 5. NPS 6. MVH 7. MTHA 8. TVA 9. NH 10. WAST 11. TCMT 12. USW 13. CTYOS 14. WCRC 15. CYC
b	Role(s) of staff responsible for	**Who by**	**Who to**	**Who by**	**Who to**	**Who by**	**Who to**

	providing and receiving the information.	1. ASB Officer & Prevent Coordinator 2. ASB Coordinator 3. Hate Crime Officer/Channel Coordinator 4. Head of Safeguarding 5. Team Manager 6. Area Housing Officer/ASB Coordinator 7. Area Housing Officer/ASB Coordinator 8. Tenancy Management Officer 9. Anti-Social Behaviour Coordinator 10. Safeguarding Lead Officer 11. Learner Welfare Services Officer 12. Director of Chaplaincy Services 13. Youth Worker 14. Team Manager 15. Learning Services Officer	3. Hate Crime Officer/Channel Coordinator	1. ASB Officer & Prevent Coordinator 2. ASB Coordinator 3. Hate Crime Officer/Channel Coordinator 4. Head of Safeguarding 5. Team Manager 6. Area Housing Officer/ASB Coordinator 7. Area Housing Officer/ASB Coordinator 8. Tenancy Management Officer 9. Anti-Social Behaviour Coordinator 10. Safeguarding Lead Officer 11. Learner Welfare Services Officer 12. Director of Chaplaincy Services 13. Youth Worker 14. Team Manager 15. Learning	1. ASB Officer & Prevent Coordinator 2. ASB Coordinator 3. Hate Crime Officer/Channel Coordinator 4. Head of Safeguarding 5. Team Manager 6. Area Housing Officer/ASB Coordinator 7. Area Housing Officer/ASB Coordinator 8. Tenancy Management Officer 9. Anti-Social Behaviour Coordinator 10. Safeguarding Lead Officer 11. Learner Welfare Services Officer 12. Director of Chaplaincy Services 13. Youth Worker 14. Team Manager 15. Learning Services Officer	1. ASB Officer & Prevent Coordinator 2. ASB Coordinator 3. Hate Crime Officer/Channel Coordinator 4. Head of Safeguarding 5. Team Manager 6. Area Housing Officer/ASB Coordinator 7. Area Housing Officer/ASB Coordinator 8. Tenancy Management Officer 9. Anti-Social Behaviour Coordinator 10. Safeguarding Lead Officer 11. Learner Welfare Services Officer 12. Director of Chaplaincy Services 13. Youth Worker 14. Team Manager 15. Learning	1. ASB Officer & Prevent Coordinator 2. ASB Coordinator 3. Hate Crime Officer/Channel Coordinator 4. Head of Safeguarding 5. Team Manager 6. Area Housing Officer/ASB Coordinator 7. Area Housing Officer/ASB Coordinator 8. Tenancy Management Officer 9. Anti-Social Behaviour Coordinator 10. Safeguarding Lead Officer 11. Learner Welfare Services Officer 12. Director of Chaplaincy Services 13. Youth

				Services Officer		Services Officer	Worker 14. Team Manager 15. Learning Services Officer
5	**Form title and reference number** Detail the title and reference number of any form(s) or letter(s) used to collect and / or convey the information.	Partnership Referral Form – see Appendix D		N/A		A support plan will be drafted.	
6	**How will the information be transferred?** Detail all agreed secure methods in which the information can be transferred to the recipient e.g. fax, direct feed from system, verbal transfer at team meeting, telephone call, e-mail.	Secure Email Verbal Telephone		Secure Email Verbal Telephone		Secure Email Verbal Telephone	

7	**When will it be shared?** Details of when the information needs to be exchanged or shared e.g. daily, weekly, monthly, yearly, as and when necessary.	As and when necessary	Quarterly meetings.	When it is deemed that someone will have on-going support following the quarterly meeting.
8	**Additional considerations** Issues or comments not included (where appropriate).			

Appendix C – Information Process Flow

Channel Panel Process Flow.docx

Appendix D – Partnership Referral Form

Partnership Prevent Referral Form.doc