Cefnogir gan
Lywodraeth Cymru
Supported by
Welsh Government

Wales Accord on the Sharing of Personal Information

Information Sharing Protocol for [Joint Intelligence Programme]

Version [Final v1.0]

Date Assured [13.10.2022]

Quality Assurance Group [South Wales WASPI QA panel]

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 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 The Joint Intelligence Programme. This is a force level joint intelligence model that allows HMPPS and the local police forces across Wales, to jointly identify (through intelligence and information sharing) the people (victims, offenders and the vulnerable), places and problems that pose the greatest threat, risk, intent, capability and harm to the local community (Local Policing Area) with specific reference to serious and organised crime. The JIP recognises the need to share information on those at risk and/or involved in organised crime at the earliest opportunity, to disrupt ongoing criminality and work collaboratively across justice services to jointly manage the risk posed effectively, ensuring that those who are vulnerable, potential victims and communities (including prison communities), are protected.

The purpose of the Joint Intelligence Programme Evaluation ('JIPE') by Cardiff University is to evaluate the process of sharing intelligence amongst police and criminal justice agencies about those at risk of embarking upon serious criminal careers.

1.4 Personal information is shared for the purpose of preventing crime and to minimise risk of harm linked to offending behaviour. Through the JIP and sharing of information/intelligence we aim to take a whole system approach to managing risk. As we are aware, offending in the community has an impact in custody and vice versa. By working together and sharing intelligence and information through the JIP, we have shown to have had an impact on maintaining prison stability and reducing crime in custody and the community. The Joint Intelligence Model has three aims:

- To jointly identifying (through intelligence and information sharing) the people (victims, offenders and the vulnerable), places and problems with specific reference to serious and organised crime that pose the greatest threat, risk and harm to the local community (BCU area) in Wales.
- To develop and coordinate pro-active local campaigns on priority risks/ threats in the area using the 4 Ps framework – (Pursue, Prevent, Prepare and Protect).
- To develop datasets that enable all aspects of the criminal justice system to have one version of the risks/threats posed by the individual or group across Wales.

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

HMPPS	Joint Intelligence Programme Analytical Support Officer	Joint Intelligence Programme (IOM)
HMPPS	Prison Intelligence Officer/Analyst or Head of Security	[to be appointed by Law Enforcement Agency (LEA)
Dyfed-Powys Police	JIP Lead Dyfed-Powys Police	[to be appointed by LEA]
Gwent Police	JIP Lead Gwent Police	[to be appointed by LEA]
North Wales Police	JIP Lead North Wales Police	[to be appointed by LEA]
South Wales Police	JIP Lead South Wales Police	[to be appointed by LEA]

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.

Table 1 - Article 6 - Personal Data

Legal basis	Check box / Notes
Task carried out in the public interest or in the exercise of official authority – Art 6(1)(e)	☒ **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 2007 Section 14** provides for disclosure by prescribed persons for the probation purposes where it is necessary and expedient to do so.

Table 2 - Article 9 - Special Categories of Personal Data

Legal basis	Checkbox / Notes
Legitimate Activities – Art 9 (2)(d)	☒ *The Criminal Justice and Court Service Act 2000 provides for a specific duty for the Police and Probation to share information in order to make joint arrangements for the assessment and*

	management of the risks posed by offenders who may cause serious harm to the public
Necessary for reasons of substantial public interest - Art 9(2)(g)	☒ 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: Schedule 1 Part 2 of the DPA 2018:- Section 6 (1) This condition is met if the processing- (a) Is necessary for a purpose listed in sub-paragraph (2) and (b) Is necessary for reasons of substantial public interest (2) Those purposes are- (a) the exercise of a function conferred on a person by an enactment or rule of law *The Criminal Justice and Court Service Act 2000 provides for a specific duty for the Police and Probation to share information in order to make joint arrangements for the assessment and management of the risks posed by offenders who may cause serious harm to the public*.

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 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:

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.

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: Administration of Justice (2).

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	☒
Gender	☒
Other reference number (eg NHS number, National Insurance number, any system/service number)	☒

6 Data Subjects' Rights

6.1 Data protection legislation provides various individual rights for data subjects. Advice on how these rights should be met should be sought from each organisation's Information Governance representative, Data Protection Officer or equivalent. Specific guidance on these rights is available on the Information Commissioner's website; www.ico.org.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
HMPPS	Website ☐ Leaflet ☒ Form ☐ Verbal ☐ Other *(specify in comments)* ☐	HMPPS Privacy Notice.pdf	n/a
Dyfed-Powys Police	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other *(specify in comments)* ☐	https://www.dyfed-powys.police.uk/hyg/fpndyfed-powys/privacy-notice/	n/a
Gwent Police	Website ☒ Leaflet ☐ Form ☐ Verbal ☐ Other *(specify in comments)* ☐	https://www.gwent.police.uk/hyg/fpngwent/privacy-notice/	n/a
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	n/a

South Wales Police	Website	☒	https://www.south-wales.police.uk/hyg/southwales/privacy-notice/	n/a
	Leaflet	☐		
	Form	☐		
	Verbal	☐		
	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 of this ISP

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
BCU	Basic Command Unit
BT PINS	The system used by HMPPS Prisons to record inmate's phone activities. This includes the lists of approved contacts and calls made.
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.
HMPPS Money Tool	The system used by HMPPS Prisons to monitor and approve inmate's financial transactions.
JIP	The Joint Intelligence Programme. This is the programme for which this WASPI was authored by and for.
JIP Case/Subject	These are references to the person who is of interest to the LEA's and HMPPS who are monitored by the JIP and discussed at the MACC meetings. They are the subjects of the data processing as in this WASPI.
LEA	Law Enforcement Agency. In this document LEA refers to all the police forces that are partner to this WASPI.

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)
MACC	Multi-Agency Conference Call. This references the monthly meetings between the JIP partners. Hosted over a secure conference phone line, it is an opportunity for LEA's and HMPPS to discuss the recent activities of the cases and discuss opportunities for intervention.
Mercury	The system used by HMPPS Prisons to record intelligence reports.
NDELIUS	The system used by HMPPS Probation to record information regarding cases.
NOMIS	The system used by HMPPS Prisons to record other information regarding to inmates that is not considered intelligence. Visitor lists and requests are available here.
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.
POM/OM	Prison Offender Manager/Offender manager (Probation Practitioner). HMPPS staff in probation who work directly with the JIP Case/Subject in either custody or in the community respectively.
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) and Section 3(4) DPA2018.
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)) Similarly, ‘Sensitive processing’ for Law Enforcement Purposes Data Protection Act 2018 is covered by section 35(8) DPA2018.

10 Appendix B – Information Reference Table for Joint Intelligence Programme

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	REFERRAL	DATA REQUEST	DATA COLLECTION	DISSEMINATION
1	**Information exchange** *General description of the process or stage to which the information sharing relates.*	The referral stage is when a subject is referred to the JIP. The subject can be referred by any of the partner agencies and can be in the community or prison. JIP subjects will be assessed by the JIP Team to confirm suitability, and then discussed at a MACC with representatives from HMPPS (OM/POM, Prison security Team, Police representatives.)	Once the subject has been discussed at the MACC a data request will be made. This will be discussed first in the MACC, and then a formal request via email will be made to the JIP Team stating clearly the data requested and the justification for it. This request will be recorded on a secure log by the Team. The request must only be relating to JIP subjects.	The JIP Team will then consider the request and if the request is relating to a JIP case and the data is obtainable, the JIP Team will collect the data by interrogating relevant systems. These will include Mercury, NOMIS, HMPPS Money tool, and BT PINS. The JIP Team will record the details of when and where the data is obtained from.	Once the data has been collected it will be shared with the representative who made the original request. The details of the dissemination will be recorded on the secure log. The data will only be shared with the requesting representative and all communications will be treated as official-sensitive. Cardiff University have agreed there will be no physical or electronic exchange of data. They will listen to the MACC meetings, but they have agreed not to record anything that identifies individuals.

	Description	REFERRAL	DATA REQUEST	DATA COLLECTION	DISSEMINATION
2	**What information will be shared?** *Describe the information to be shared – you do not need to go to 'field level' detail.* ***Please note**: **Only the minimum and relevant personal information is to be shared and strictly on a case by case basis.***	The referral will contain identifiers including • Name • Date of Birth • Gender • PNCID • NOMIS number • CRN These will be supplied to the JIP by the person making the referral for the basis of beginning the initial assessment. The initial assessment will require the interrogation of HMPPS systems. The profile will be disseminated to relevant partners containing the above data as well as • Current address • Current location (prison/community) • OM details • Summaries of case notes and available intelligence. Please note that at this time all information is treated as official-sensitive.	The data request will require the identifiers listed in the referral section to confirm the subject that the request is related to. • Name • DoB • Gender • One other identifier And also the specific data required for the request: • BT PINS Contact List • HMPPS Money Tool data • HMPPS Mercury • HMPPS Visits	At this point the JIP Team will collect the requested data. This can include • Phone contacts from BT PINS • Transactions made via HMPPS Money Tool • Intelligence around the subject from Mercury • HMPPS Visits This info will be collected by the JIP Team and stored securely prior to dissemination.	The data collected by the JIP Team will then be shared with the data requester. The information shared is the same as that collected in the Data Collection section.

	Description	REFERRAL		DATA REQUEST		DATA COLLECTION		DISSEMINATION	
3	**Partner Organisation(s)** *Details of provider and recipient organisation(s)* *Ensure the organisations listed reflect section 2 of the ISP i.e. are all organisations listed in section 2*	**Who by**	**Who to**	**Who by**	**Who to**	**Who by**	**Who to**	**Who by**	**Who to**
		HMPPS Probation Staff (OM/POM) HMPPS Prison Staff (intelligence Analyst/Head of Security) LEA Police representative	HMPPS Joint Intelligence Programme	HMPPS Prison Staff (intelligence Analyst/Head of Security) LEA Police representative HMPPS Offender Managers Approved Researchers (Cardiff University)	HMPPS JIP Team	HMPPS JIP Team	n/a	HMPPS JIP Team	Requesting Partner Cardiff University

	Description	REFERRAL	DATA REQUEST	DATA COLLECTION	DISSEMINATION
4	**How is information shared and what methods are used to keep the information secure?** *Provide, in detail the specific agreed secure methods for sharing personal information*	The referral will be made via email. Any person working for the JIP Partners can submit a request for assessment. The data relating to the referral will also be shared via secure TLS enforced email so that an assessment can begin.	Please note that data requests at this stage for specific data and intelligence can only be made by approved partners. The data request will be made via email. Details of the request including who's made the request, dates, and the data requested. The details of the request will be saved on a password protected Excel Spreadsheet on a MoJ approved Quantum laptop. This laptop is accessed solely by the JIP TEAM and is stored securely between uses. The Quantum laptop is protected by BitLocker, Pulse Secure and RSA Security ID software, and password protected Citrix software. In the event that the Quantum laptop is loss BitLocker software will prevent unauthorised access and procedures are available for wiping the laptop should the BitLocker be broken and should the laptop connect to a network.	BT PINS contact records will be accessed via a dedicated computer located in the RIU. Data from Mercury, NOMIS, HMPPS Money Tool will be collected from the relevant systems via a Quantum Laptop. Data will then be saved on the Quantum Laptop and password protected and stored for 3 months from the date of collection. even after dissemination. Data collected will first be interrogated by the JIP TEAM who will use this data to keep records on JIP Subjects updated and to develop intelligence. Further research into the data will also be conducted at this point as needed, such as research into new persons/objects found within the data relating to the JIP subject.	The data will be disseminated via email to the requester via secure TLS enforced email. It will be marked as official-sensitive and the files will be compressed into a password protected Zip file. Once disseminated, it is the responsibility of the person receiving the data to further adhere to data protection guidelines to ensure the security of the received data. The Joint Intelligence Programme is required to ensure effectiveness for all partners. Cardiff University have been commissioned to complete this. This research has been approved by the NRC reference 2021-214. No physical data will be shared with Cardiff University. Cardiff University will attend and observe meetings where personal details of individuals discussed would be shared verbally. Researchers will not record, retain or store these details for any purpose. A Memorandum of Understanding has also been agreed between HMPPS as the commissioning authority for the research, and Cardiff University. JIPE Memorandum of Understanding.doc NRC letter 2021-214.doc

	Description	REFERRAL	DATA REQUEST	DATA COLLECTION	DISSEMINATION
5	**Reliance on consent** *Check the box if any exchange relies on consent and explain how and when consent is obtained. Ensure section 4 of the ISP reflects this legal basis*	☐ Exchange relies on consent ☒ Exchange does not rely on consent	☐ 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
6	**Notes for Practitioners**	The referral stage is to ensure that the subject is suitable for the JIP. This stage is standard for all persons referred to the JIP. In relation to this WASPI, the referral confirms eligibility of persons into the JIP, and therefore confirming eligibility of the data sharing pertinent to this WASPI.	Data requests will only be relating to JIP subjects. Data requests for data relating to non-JIP subjects will be rejected by the JIP. The MACC meeting itself relies on verbal voluntary disclosure. These are monthly meetings in which updated information around JIP subjects are shared by HMPPS and the LEA's. It is at the MACC that discussions are had around the data required between partners, which will then be formalised by the partners in the data request email.	Data collected will be necessary and proportional to the request. Data collected will firstly be processed by the JIP TEAM. The JIP TEAM will use the data to update JIP subject records and to develop	Please note the password will be sent in a separate email.