Ministry of Justice

HM Prison & Probation Service

Policy name: HMPPS Information Sharing Policy Framework

Re-Issue Date: 26 May 2023 **Implementation Date:** 28 May 2021

Replaces the following documents (e.g. PSIs, PSOs, Custodial Service Specs) which are hereby cancelled:

- PSI 16/2016, AI 12/2016, PI 15/2016 Information Sharing Policy

Introduces amendments to the following documents: N/A

Action required by:

☒	HMPPS HQ	☒	Governors/Directors
☒	Public Sector Prisons	☒	Heads of Group
☒	Contracted Prisons	☒	Central Contract Managers
☒	National Probation Service	☒	Relevant Supply Chain Providers
☒	HMPPS Rehabilitation Contract Services Team	☒	HMPPS-run Immigration Removal Centres (IRCs)
☒	Other providers of Probation and Community Services	☒	Under 18 Young Offender Institutions
☒	Youth Custody Service		

Mandatory Actions: All groups referenced above must adhere to the Requirements section of this Policy Framework, which contains all mandatory actions.

For Information: All Information Asset Owners, Information Asset Custodians, Senior Managers, Delivery Partners and Third Party Suppliers.

How will this Policy Framework be audited or monitored: Mandatory elements of instructions must be subject to management checks and may be subject to self or peer audit by operational line management/contract managers/HQ managers, as judged to be appropriate by the managers with responsibility for delivery. In addition, HMPPS will have a corporate audit programme that will audit against mandatory requirements to an extent and at a frequency determined from time to time through the appropriate governance.

Resource Impact: Any information sharing identified as occurring at a local or regional level will be addressed as a 'business as usual activity' by all teams that this framework is applicable to.

Any shares identified as occurring at a national level will be the responsibility of the HMPPS Information Security (InfoSec) and Services Team to facilitate the signing of these documents with the HMPPS Senior Information Risk Owner (SIRO).

Contact: informationmgmtsecurity@justice.gov.uk

Deputy/Group Director sign-off: Ian Blakeman, Executive Director, Performance Directorate, Directorate of Strategy Planning and Performance

Approved by OPS for publication: Ian Barrow and Sarah Coccia, Joint Chair, Operational Policy Sub-board, May 2021

Revision

Date	Change
26 May 2023	Minor amendment, page 4 section 1

CONTENTS

Section	Title	Page
1	Purpose	4
2	Outcomes	4
3	Requirements	4-8
3.1	What is Information Sharing?	4-5
3.2	Scope	5
3.3	Who are the key players?	5-6
3.4	Types of Information Sharing Agreements (ISA)	6-7
3.5	Types of sharing	7-8
4	Guidance	8-9
4.1	The process for creating an agreement for a new instance of personal data sharing	8-9
4.2	The process for creating an agreement for an existing instance of personal data sharing not already covered by an agreement	9
5.	WASPI	10
Annex A	Section 14, Offender Management Act 2007	10-11

1. Purpose

The purpose of this framework is to recognise that the sharing of personal data is a process integral to meeting the HMPPS business objectives. This framework provides guidance and support to practitioners in establishing agreements to make the process as straight forward as possible. Any sharing of personal data – whether small or large scale – needs to be done in accordance with the provisions of the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR). The DPA provides a framework for how personal data should be correctly handled. The DPA neither promotes nor prohibits the sharing of personal data, but its principles apply to data sharing as they apply to any other form of processing of personal data.

Following a Cabinet office review, it has been agreed that a Memorandum of Understanding (MOU) will suffice between Government Ministries instead of an Information Sharing Agreement (ISA). The MOU should cover all aspects of the data sharing arrangement between the Government Ministries however a legally binding ISA is not required.

2. Outcomes

The framework sets out HMPPS's commitment to the management of information sharing. It also sets out what Prison Establishments (including under 18 YOIs sites), Probation Regions, Headquarters Groups and all relevant supply chains should do to manage information sharing. In doing so, this policy supports the wider HMPPS strategic aims and objectives and should enable employees throughout the organisation to establish information sharing agreements.

3. Requirements

3.1 What is Information Sharing?

Prison Establishments (including under 18 YOIs) Probation and HQ share information with a variety of stakeholders in order to achieve specific goals. For example, in an establishment information is shared with charities that assist in the rehabilitation of offenders. Probation shares information with private providers and charities that assist Offenders with housing and accommodation needs. HQ shares information with researchers for a number of purposes e.g. to understand through research how re-offending can be reduced.

Section 14 of the Offender Management Act 2007 (**Annex A**) sets out the powers of certain bodies to share data for specified purposes.

In the context of this Policy Framework the term information sharing is defined as the process of sharing any personal data, using a method that ensures compliance with the principles of the DPA 2018 and the guidance provided by the Information Commissioners Office (ICO) to ensure the share is lawful. These principles are;

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

In the context of this policy the term 'agreement' is used in reference to an 'Information Sharing Agreement' or ISA. An ISA is a document which sets out when and how information should be shared and stored and the relevant safeguards that must be adopted in order to ensure safe processing of that data.

Agreements will reduce the risk to information that can occur when information is not shared correctly or without adequate controls in place. In addition to complying with the data protection principles, these matters that need to be considered fall into three main categories:

- Confidentiality means ensuring that only authorised people can access our information.
- Integrity means ensuring that it is authentic, accurate and complete.
- Availability means that authorised people can access it when they need to, at the right times in the right ways.

3.2 Scope

This policy details the controls required when sharing personal data with third parties, who have no prior sharing agreement or contract with HMPPS.

The policy does not cover sharing detailed in PSI 03/2018, The Data Protection Act 2018, Freedom Of Information and Environmental Information Regulations, such as sharing data upon receipt of a Court Order or requests made by Offenders for their personal data made as subject access requests.

The policy in no way hinders staff from sharing personal information in order to prevent abuse or serious harm. However, Prison Establishments (including under 18 YOIs) and Probation must ensure that details of an individual offenders spent convictions, including any offence related information that might be used for risk assessment, are not disclosed to **any** Local Authority or Third-Party organisation unless that person can justify that they are entitled to that information in accordance with the provisions of the Rehabilitation of Offenders Act 1974 regarding spent convictions. Guidance relating to the sharing of the OASys Assessment are covered within the OASys Guidance: Sharing the OASys, Assessment issued in April 2015.

The policy assumes that no contract exists between the parties taking part in the share. If a contract is in place it is preferable to define information sharing within it rather than as a separate document. If you have a contract in place but are not confident that sufficient coverage is provided for the sharing of information please contact the HMPPS Information Security (InfoSec) & Services Team for advice: informationmgmtsecurity@justice.gov.uk.

3.3 Who are the Key Players?

National HMPPS agreements must be signed by the Senior Information Risk Owner (SIRO), Information Asset Owners (IAOs), or delegated authorities who are responsible for the risks associated with the share as owners / custodians of the personal data.

All other agreements within the supply chain will need to be signed by a senior individual within that organisation.

These individuals, through delegated authority assume the role and responsibilities of the "Data Controller". The DPA defines this role as "… a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed".

According to the definition in the DPA, a data controller or data controllers must decide the purposes for which, and the way in which personal data are, or will be, processed. The Information Commissioner's Office's (ICO) view is that the determination of the purposes for which personal data are to be processed is paramount in deciding whether or not a person is a data controller and that when a person determines the purposes for which personal data are to be processed, a decision as to the manner in which the data is to be processed is often inherent in that decision.

The Ministry of Justice (MoJ) is the registered Data Controller for HMPPS data. Therefore, all agreements will be between the Secretary of State for Justice (as the Minister responsible for the MoJ) and third parties. However, the individuals who sign the agreements on behalf of the Secretary of State will differ according to the type of agreement.

For agreements established at a national level (defined in 3.5 as Type 1), it is the Secretary of State for the MoJ who has delegated authority to the HMPPS SIRO.

For agreements established at a regional level (defined in 3.5 as Type 2), authority is delegated from the HMPPS SIRO to the Prison Group Director (PGD) and Regional Probation Directors.

For agreements established at a Prison Establishment (including under 18 YOIs) / Probation Delivery Unit (PDU) Cluster level (defined in 3.5 as Types 3 and 4), authority is delegated from the HMPPS SIRO to Prison Governors / Directors (Private Prisons) and Regional Probation Directors, and may be further delegated as appropriate.

For agreements established by HQ the signatory will be the HMPPS SIRO or their deputy (Type 1).

3.4 Types of Information Sharing Agreements (ISA)

There are two main categories of agreement;

- Agreements between Data Controllers, these can be either;

    1. ISAs between public sector data controllers which can be in the form of a non-binding MoU; and

    2. legally binding ISAs between MoJ/HMPPS and non-public sector data controllers.

- Agreement between Data Controllers and Data Processors. This type of an agreement is a data processing agreement and must be covered as part of the contract between the Data Controller and Data Processor.

A template has been provided for an agreement between Data Controllers which can be found on the HMPPS Information Security (InfoSec) & Services Team intranet support page (**link**). Additional guidance for completing this template can be sought from the HMPPS Information Security (InfoSec) & Services Team (informationmgmtsecurity@justice.gov.uk). For Data Controller to Data Processor arrangements a contract must exist that sets out the data processing requirements (including Information Sharing).

The DPA defines a data processor, in relation to personal data, as "any person (other than an employee of the data controller) who processes the data on behalf of the data controller." This

means that the person processes data for a purpose and according to a manner determined by the data controller and makes no independent determination of such matters.

The DPA introduces specific obligations upon data controllers when the processing of personal data is carried out on their behalf by data processors. The data controller retains full responsibility for the actions of the data processor and so the definition of data controller is important in this context.

Agreements between Data Controllers and Data Processors must form part of a contractual agreement (unless the agreement is between Government departments), in such instances advice should be sought from: informationmgmtsecurity@justice.gov.uk

Ad-Hoc data sharing i.e. a small scale, non–routine, or one-time sharing of information will not normally require an agreement to be in place. However, when data is shared in this way compliance with the DPA and HMPPS Information Security (InfoSec) & Services policies is still required. The decisions and requirements should be documented, and the document retained for reference. A 'Memorandum of Understanding' may be appropriate for this. Advice can be sought from informationmgmtsecurity@justice.gov.uk.

3.5 Types of Sharing

Four types of sharing have been identified, depending on the scale of its application:

Type 1 agreements can only be signed off by the HMPPS SIRO or their deputy.

Type 1	This covers agreements where at least one of the signatories is at Departmental (MoJ) level. An example of an agreement at this level is the one between MoJ and NHS England for healthcare services. Responsibility for creating and maintaining this agreement type will be with HMPPS HQ. The HMPPS SIRO (or their delegated authority) would be the agency signatory. Any agreement drawn up by a HMPPS HQ department will also fall within this category.

Type 2 agreements can only be signed off by the regional PGD or Regional Probation Director.

Type 2	This would cover agreements where one supplier is providing the same service to a number of establishments or PDU's. A custody example would be where a university provides a skills service to all the establishments within its area. Responsibility for creating, maintaining and signing this agreement type will be with the Prison Group Director for the pertinent region (or their delegated authority), or the Regional Probation Director (or delegate) for their Region, with advice and guidance being given from HQ informationmgmtsecurity@justice.gov.uk

Type 3 agreements can only be signed off by the Establishment Governor/Director (Private Prisons only), or Regional Probation Director (or delegated authority).

Type 3	This would cover agreements where one supplier provides services to one Prison establishment (including under 18 YOIs) or one/many offices within a Probation PDU. A community example could be where a private provider offers drug test services within the County only. Responsibility for creating and maintaining this agreement type will be with the establishment or PDU's, with advice and guidance being given from HQ. The establishment Governor/ Director (Private Prisons only) (or their delegated authority), or Regional Probation Director (or their delegated authority) would be the signatory.

Type 4 agreements can only be signed off by the Establishment Governor/Director (Private Prisons only), or Regional Probation Director (or delegated authority).

Type 4	As with a Type 3 agreement but with the exception that a standard agreement template will be drawn up by HQ. An example is where healthcare provision is commissioned nationally but the delivery is via a local supplier. Appropriate signatories will be identified as part of the guidance. Establishments (including under 18 YOIs) and Probation should note that where access to core applications e.g. P-NOMIS/National Delius/YJAF is granted to non HMPPS staff an agreement should always be considered, except where they are non-directly employed staff subject to the same vetting as directly employed staff.

Any business unit considering establishing or renewing a Type 1 or Type 4 agreement must in the first instance contact informationmgmtsecurity@justice.gov.uk to discuss.

4. Guidance

4.1 The process for creating an agreement for a new instance of personal data sharing

Any party wishing to initiate information sharing with HMPPS must firstly fill in a 'Data Request Form'.

A sample Data Request Form can be found on the HMPPS Information Security (InfoSec) & Services Team intranet support page (**link**). It is important to complete the Data Request Form as fully as possible as it will form the basis for the agreement. It also ascertains as early as possible whether HMPPS can supply the required data.

Once the 'Data Request Form' has been completed, the Data Privacy Impact Assessment (DPIA) process must be followed.

The process of performing a DPIA firstly involves the completion of a screening questionnaire to ascertain whether a DPIA is or isn't required. This needs to take place via the MoJ One Trust system, where all DPIAs are stored. Once completed, the process will highlight the risks associated with the share. The risk register, defined by PSI 6/2016 (PI 8/2016) -Information Risk Management Policy - can be used to document the risks. Guidance on completion of the DPIA process can be found on the HMPPS InfoSec & Services Team website (**link**).

All risks associated with an information share must be documented and presented to the agreement signatory (as identified in section 3.3). The process of establishing the share can

only progress once the signatory has accepted the risks identified and all mitigating privacy controls have been identified.

Once authorisation has been received to progress with the information sharing, the appropriate ISA template should be completed to detail the specifics of the share.

All sharing of personal data applicable to this policy must be captured using the appropriated mechanism as discussed in section 3.2.

Once an agreement is in place and the share is authorised to take place it should be recorded in the appropriate Information Asset Register (IAR) (either the Establishment register, Probation Regional register, or the HQ Directorates register). For advice, contact your Local Information Manager (LIM).

All agreements are subject to a minimum annual review. The responsibility for reviewing will depend upon the level of agreement as defined in section 3.5.

The agreement signatory is responsible for ensuring that there is a process in place to ensure that the agreement is reviewed in accordance with the period detailed within the agreement.

4.2 <u>The process for creating an agreement for an existing instance of personal data sharing not already covered by an agreement</u>

It is recognised that, at the introduction of this policy, there may be some instances where information is shared but that the share is not covered by an appropriate agreement. It is expected that the process of establishing an agreement is to commence at the earliest opportunity.

Any sharing of personal data, as defined by this policy, not covered by an appropriated agreement must be recorded on a risk register.

Where sharing of personal data is already in progress but not covered by an appropriate agreement the ICO recommends "…that projects which are already up and running are not submitted to a DPIA process, but to either a compliance check or a data protection audit, whichever is more appropriate."

When establishing an agreement for an existing information share the same process is advised as detailed in section 4.1 however instead of following the DPIA process, a "Data Sharing Compliance Checklist" should be completed. A copy of the Data Sharing Compliance Checklist can be found on the HMPPS Information Security (InfoSec) & Services Intranet Support page (**link**).

If a routine share is in place without an ISA or MOU (for sharing between Government Ministries) MOJ/HMPPS could be at risk of sharing information unlawfully and this should not be normal business practice therefore requires to be rectified immediately.

Assistance and guidance, if required, for Supply Chain Providers of Services, in relation to Information Sharing, can be sought from the HMPPS Information Security (InfoSec) & Services Team via their functional mailbox; Informationmgmtsecurity@justice.gov.uk.

5. Welsh Accord on the Sharing of Personal Information

The Welsh Accord on the Sharing of Personal Information (WASPI) is a region-specific agreement in HMPPS in Wales. Either the WASPI template or the HMPPS template will offer a suitable framework on which to develop an agreement for the sharing of HMPPS information in Wales. The WASPI lead team based in the NHS can provide quality assurance support for use of the WASPI template, as to can the policy holders for the HMPPS template.

Annex A

Section 14 Offender Management Act 2007

(Disclosure for Offender Management Purposes)

Section 14 of the Offender Management Act 2007 sets out the powers of certain bodies to share data for specified purposes. There are two lists set out in the Act as set out below.

List A

(a) the Secretary of State;

(b) a provider of probation services (other than the Secretary of State);

(c) an officer of a provider of probation services; and

(d) a person carrying out activities in pursuance of arrangements made by a provider of probation services […].

List B

(a) a government department;

(b) a relevant local authority;

(c) the Youth Justice Board for England and Wales;

(d) the Parole Board for England and Wales;

(e) a relevant contractor*;

(f) a chief officer of police;

(g) a person who is responsible for securing the electronic monitoring of an individual; and

(h) any other person specified or described in regulations made by the Secretary of State.

* "Relevant contractor" means those contracted to provide prison, young offender institution, secure training centre and related escort services are within the ambit of the section.

Those in list A are permitted to share data with one another. It also enables disclosure between those bodies and the bodies listed in List B. However, data sharing is not authorised between those bodies in List B (although there may be powers outside of the Offender Management Act 2007 that authorise this).

This power to share is only permitted if the disclosure is necessary or expedient for the following purposes:

- The probation purposes (section one Offender Management Act 2007)
- The performance of the functions relating to prisons or prisoners of:
  - The Secretary of State;
  - Any other person to whom section 14 applies; or
  - Any listed person; and
- Any other purpose connected with the management of offenders (including the development or assessment of policies relating to matters connected with the management of offenders).

The section 14 power further provides that the meaning of “functions, prisons, and prisoners” includes that young offender institutions and secure training centres, together with those persons detained within them, are treated as prisons or prisoners respectively for the purposes of this clause.

The power to exchange information by virtue of this section does not affect any existing power to share data that exists independently of the section and that any such exchange is subject to existing safeguards regarding the sharing of data.