PROCESS-SPECIFIC DATA SHARING AGREEMENT (PDSA)

In respect of

Access to HM Passport Office data in relation to the Data Validation Application Digital (DVA: Digital) User Interface (UI)

subject to the

OVERARCHING UMBRELLA DATA SHARING AGREEMENT (UDSA) V4.0 between

The Secretary Of State For The Home Department,

The National Police Chiefs' Council (On Behalf Of Police Forces Of England & Wales),

The Police Service of Scotland,

The Police Service of Northern Ireland,

And

S.23(1) [redacted]

1	Summary and Version Control
Title	Northumbria Police – Force Intelligence Bureau (FIB) and HM Passport Office On behalf of THE HOME OFFICE Access to HM Passport Office data in relation to the Data Validation Application Digital (DVA: Digital) User Interface (UI)
Author(s)	Lauren Smith – HM Passport Office, Data Governance & Assurance Team
Next Review Date	[Insert date of next review – review intervals should be listed in Administration below.]
Date Issued	[Insert date the PDSA comes into effect (this is usually the date of final Participant signature).]
Disclosure	This document is not suitable for disclosure to organisations other than the participants. This document is not suitable for publication.
Retention Date	N/A while processing is ongoing
Classification Marking	OFFICIAL

Version control			
Version	**Date**	**Amended by**	**Summary of Changes**
v0.1	20th March 2025	HM Passport Office	Initial draft

2 Contents

3 Introduction

3.1 A Process-Specific Data Sharing Agreement (PDSA) is an information sharing document which is approved and signed by the Participants listed in Schedule 1 of the Umbrella Data Sharing Agreement (UDSA).

3.2 The UDSA sets out the high-level arrangements that govern the sharing of information between the UDSA Participants. The UDSA requires that all participants comply with UK Data Protection Legislation and associated governance arrangements in the course of this Data Sharing Activity. The Data Protection obligations placed upon the participants within the UDSA will also be adhered to under the PDSA.

3.3 This PDSA is made under the terms of the overarching UDSA between the Home Office (HO), National Police Chief's Council (NPCC), Police Service of Scotland known as Police Scotland (PS), Police Service of Northern Ireland (PSNI), S.23(1) Any Personal Data shared pursuant to this PDSA is subject to the provisions set out in the UDSA and should be read in conjunction with it.

3.4 This PDSA is not a contract nor is it legally binding. It does not in itself create a lawful means for the exchange of information; but rather documents a framework of the information sharing processes and procedures the Participants agree to work within.

3.5 This document does not impose a duty to disclose data, nor does it provide the power to demand disclosure.

3.6 Under this agreement data sharing between the Participants is considered to be on a Controller-to-Controller basis.

4 Participants

4.1 Collectively the organisations listed below will be referred to as the "Participants" and individually as a "Participant":

- The Home Office of 2 Marsham Street, London, SW1P 4DF
    - The operational participant on behalf of the controller will be HM Passport Office on behalf of the Home Office, hereafter referred to as HMPO throughout this document.
- Northumbria Police Force Intelligence Bureau, Etal Lane Police Station, Newcastle Upon Tyne, NE5 4AW
    - The operational participant will be Northumbria Police Force Intelligence Bureau hereinafter called the receiving Law Enforcement Agency (LEA).

5 Data Sharing Activity and Purpose

5.1 The information sharing activity outlined in this PDSA involves regular sharing of Personal Data between the Home Office and the receiving LEA as independent controllers.

5.2 The Participants have identified the following necessity, purpose(s), and benefits for the data sharing activity described in this PDSA:

Purpose

DVA: Digital will be accessed by the receiving LEA on a case-by-case basis, where it is necessary and proportionate to do so for law enforcement purposes which are defined in section 31 UK Data Protection Act 2018 as: "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."

DVA: Digital may also be used by the receiving LEA where necessary and proportionate for the purposes of protecting life and property, preserving order, preventing and detecting offences, bringing offenders to justice and any duty or responsibility arising from common law or statute as set out in the College of Policing's Information Management Authorised Professional Practice.

More specifically DVA: Digital may be used as one of many intelligence sources to assist in the identification of suspects and their associates, victims, and witnesses across a range of operational policing activities.

Schedule 1 defines the teams/units within the receiving LEA whose usage of DVA: Digital has been agreed.

Benefits

From a policing perspective the sharing will help achieve the purposes described above which are beneficial for the public as a whole. Additionally, those benefits will help increase the public's trust and confidence in the Police, something fundamental to the UK policing model.

6 Approved Data

6.1 The Participants decide to share the data listed in the Table in 'Schedule 1 – Personal Data to be shared' (together 'the Approved Data').

Home Office

6.2 A DPIA to assess the risks of data sharing with Law Enforcement organisations has been completed and approved by the Office of the Data Protection Officer on the 4th May 2022. An application form relating to the receiving LEA's access to HMPO's data has been approved by HMPO on 2nd July 2013 which forms part of this PDSA review.

The Receiving LEA

6.3 It is the responsibility of the receiving LEA to consider completion of a DPIA, as needed, in order to meet UK Data Protection obligations. Confirm if a DPIA has been completed and insert the date that it was completed.

7 The Data Sharing Process

This section further outlines compliance with the Data Minimisation & Accuracy Principles.

7.1 Data will be shared and protected as follows:

Reliance on Personal Data for the Information Sharing Activity

Data accessed via DVA: Digital is generally used by the police to corroborate other sources of police intelligence rather than being the sole source. Data accessed via DVA: Digital is valuable to confirm the identity of suspects, offenders, victims, and witnesses whose identity is not otherwise confirmed to police forces and all other sources of Police intelligence have been exhausted.

Volume

This activity relates to access to Passport data through the DVA: Digital UI, the receiving LEA's access to this data will be on a case-by-case basis, as such volumes will vary.

Duration

This is an on-going data sharing agreement.

Source(s) of the data/information

This data is stored on a HMPO database and provided via the DVA: Digital UI.

Frequency

On a case-by-case basis.

Format

Passport data is accessed via DVA: Digital UI. DVA: Digital UI is a means by which public sector organisations can securely access passport data on a read-only basis via a web browser, no data is physically transferred or moved.

Accuracy of the shared data

HMPO has appropriate measures in place to ensure that the data they hold is accurate and up to date in accordance with the UK Data Protection Legislation. In circumstances where the recipient of the information is intending to use the information to make a decision that will impact directly on the data subject, the receiving LEA must be satisfied that there is sufficient and accurate information available to them before making a final decision and should always seek to clarify, or make further enquiries with the data subject, or with HMPO in the event that a decision is subsequently disputed/appealed by the data subject.

Notification and rectification of errors in the data/Information shared If any inaccuracies are discovered HMPO will update it's records, however they will not separately notify the receiving LEA.
Rectification If any inaccuracies are discovered HMPO will update its records.

Data Security

This section outlines compliance with the Integrity and Confidentiality Principle.

Security Standards

7.2 The receiving LEA acknowledges that HMPO places great emphasis on confidentiality, integrity, and availability of information and consequently on the security of the receiving LEA's sites and the security for the receiving LEA's systems and procedures. The receiving LEA also acknowledges the requirement to maintain the confidentiality of HMPO's data.

7.2.1 The receiving LEA shall be responsible for the security of its system and shall at all times provide a level of security which:

(i) is in accordance with Good Industry Practice (such as ISO27001), the Government Functional Standard GovS 007: Security Standard and related standards and Law;

(ii) is commensurate with the threats to the receiving LEA's system;

7.2.2 Without limiting the above paragraph the receiving LEA shall at all times ensure that the level of security employed in accessing HMPO's data is appropriate to manage the risks associated with the following:

(i) loss of confidentiality of HMPO's data;

(ii) unauthorised access to, use of, or interference with HMPO's data by any person or organisation; and

(iii) use of the receiving LEA's system by any third party in order to gain unauthorised access to any computer resource or HMPO's data.

7.2.3 The receiving LEA shall comply with any security operating procedures/acceptance use policy (AUP) or instructions provided by HMPO, and any further standards, guidance and policies and any successor to or replacement for such standards, guidance, and policies, as notified from time to time.

7.2.4 the receiving LEA shall comply with the declarations made and obligations undertaken in the DPIA it completed to receive HMPO's data.

7.2.5 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the receiving LEA should notify HMPO of such inconsistency immediately upon becoming aware of the same, and HMPO shall, as soon as practicable, advise the receiving LEA which provision they shall be required to comply with.

7.2.6 In receiving HMPO's data the receiving LEA agrees to:

i. Ensure that there are adequate protective security measures in place to ensure the safeguarding of the storage, transmission or processing of HMPO data;

ii. Limit access to HMPO data to those persons required to carry out functions under this PDSA save for where onward transmission is consistent with statutory or common law powers, in which case the agreement of HMPO must be sought;

iii. Ensure any actions taken in respect of HMPO's data are in accordance with UK Data Protection Legislation;

iv. Ensure that HMPO's data is protected from unauthorised dissemination, and unauthorised or unlawful processing, and against accidental loss or destruction of, or damage to, personal data;

v. Have in place procedures or processes to minimise the risk of unlawful extraction of HMPO's data provided under this PDSA, including the control of removable media and data storage devices as required;

vi. Ensure that all of its personnel with access to HMPO's data:

a. have undergone Staff Vetting procedures
b. have read the Security Operating procedures/Acceptable Use Policy (AUP)
c. are trained in the safeguards required to protect such information and in the restrictions on the use and dissemination of such information
d. are only allowed access to HMPO's data from official corporate devices that have been assured
e. only access HMPO's data from secure, official premises unless otherwise agreed with HMPO.
f. are adequately supervised by the receiving LEA

7.2.7 the receiving LEA will ensure that there is auditable evidence that such safeguards are being applied;

7.2.8 The receiving LEA will ensure that there are robust processes in place to remove access to HMPO's data for staff that no longer requires such access.

7.2.9 The receiving LEA will notify HMPO without delay

i. of any situation that disrupts the intended transfer of information to the receiving LEA,

ii. if it appears that any appropriate electronic, physical and /or procedural safeguards may or have been compromised, or

iii. if it becomes aware of any attempt to effect such compromise in respect of any HMPO's data; and

7.2.10 The receiving LEA will take appropriate action, in accordance with administrative, civil and criminal laws, in the event of misuse, unauthorised alteration, deletion of or access to or dissemination of HMPO's data by the receiving LEA personnel or any third party.

7.2.11 The receiving LEA will ensure that there are adequate protective security measures in place to ensure the safeguarding of the storage, transmission or processing of data provided to the receiving LEA under this agreement and that any such measures have been assessed and agreed as appropriate by HMPO.

7.2.12 The receiving LEA will delete immediately on receipt any information received from HMPO which is not required for the 'Authorised Purpose' and only retain HMPO's data for as long as is necessary.

7.2.13 The receiving LEA will have a written contract with any agent it uses to carry out functions on its behalf, notified to HMPO in advance of the commencement of that contract, the terms of which in respect of the data protection measures relating to the processing of the information for the 'Authorised Purpose' are no less stringent than the terms set out in this PDSA. In the event that the receiving LEA makes or intends to make any changes to the contract, it will notify HMPO in advance of any such changes being made and ensure that any such changes will not render the contract any less stringent than the terms set out in this PDSA.

7.2.14 The receiving LEA will ensure:

i. that all access to the receiving LEA's data is controlled and limited to appropriately vetted persons authorised to have access to HMPO's data and that all such access is logged and monitored, and that any irregularities of access are reported immediately to HMPO and investigated.

ii. that all HMPO's data obtained is handled in accordance with UK Data Protection Legislation.

iii. that all aspects of the receiving LEA's business which involve processing HMPO's data are conducted in accordance with the mandatory requirements of the Government Functional Standards: GovS 007 Security and related standards and guides.

Standard Operating Procedures

7.2.15 Data Access Services will:

- will manage the initial set up of the receiving participant onto DVA: Digital
- and act as the single contact point in the event of systems issues relating to DVA: Digital

i. DVA: Digital UI incorporates role-based access via three different type of customer accounts:

1) Standard user account.

Allows passport data searching.

2) Organisation Administrator (with license) user account.

Allows passport data searching, but with the additional functionality of Standard user account management such as creating, amending, unlocking and deleting Standard user accounts for users within the Organisation Administrator's team.

3) Organisation Administrator (without license) user account.

An administrative only role, allowing Standard user account management only.

ii. HMPO will create accounts for each member of the receiving LEA's personnel who they wish to have the Organisation Administrator role, as notified by the Participant.

iii. Organisation Administrators are responsible for maintaining any Standard user accounts as needed under the terms of this PDSA.

iv. Creating an account will trigger DVA: Digital to auto email the user with a unique username and first-time password to enable each member of the receiving LEA's users to log on to the DVA: Digital System and activate their account.

7.2.16 DVA: Digital is designed to provide a response time of 95% within 5 seconds.

7.2.17 The above target response time is from the point at which DVA: Digital receives the query to the point at which DVA: Digital sends a response. The times experienced by the receiving LEA may be longer if there are delays outside of the infrastructure controlled by HMPO or if there is an incident.

7.2.18 DVA: Digital will be available for use by the receiving LEA 24 hours a day unless planned maintenance is scheduled, which HMPO will, wherever possible, schedule to take place between 22:00 on a Saturday and 06:00 on a Sunday. Where this activity affects the availability of DVA: Digital, HMPO will provide a minimum of 5 working days' notice to enable the receiving LEA to explore contingency options. Once internal approval has been granted for the maintenance to take place HMPO will provide notification by email to the receiving LEA's nominated contacts.

7.2.19 In the event of unplanned system downtime HMPO will inform the receiving LEA's nominated contacts by email as soon as it is aware of the issue. It will provide an estimate of any time that DVA: Digital will be unavailable and will continue to send email updates at regular intervals until the incident is resolved. Such notification will only be provided between the periods Monday – Friday 9am – 5pm UK local time, excluding public holidays and is subject to the receiving LEA having provided HMPO with details of nominated contacts.

7.2.20 In the unlikely event of intrusion detection DVA: Digital will be suspended immediately, and the receiving LEA's nominated contacts will be informed as above.

7.2.21 HMPO will endeavour to make available an alternative connection in the event of suspension or closure of DVA: Digital.

7.2.22 DVA: Digital infrastructure incidents raised with HMPO will be prioritised as follows:

Description **DVA: Digital Infrastructure Incident**	Incident Priority	Action Time
Incident is business threatening	P1	4 hours
Two or more customers are impacted	P2	8 hours

Users experiencing reduced system performance	P3	5 working days
Fault other than defined above	P4	15 working days

7.2.23 DVA: Digital application incidents raised with HMPO will be prioritised as follows:

Description	Incident Priority	Action Time
DVA: Digital Application Incident		
Incident is business threatening	P1	2 hours
Two or more customers are impacted	P2	4 hours
Users experiencing reduced system performance	P3	10 Business Days
Fault other than defined above	P4	20 Business Days

7.2.24 The incident priority is determined by HMPO, and these response times are on a reasonable endeavour's basis. During business hours HMPO will provide a communication acknowledging the incident to the receiving LEA within 1 hour of being notified of the occurrence. Outside of these hours will be on a reasonable endeavour's basis. If the incident has not been resolved by 10pm on a working day, the clock stops, and any remedial work is suspended until 8:30am on the following working day.

7.2.25 HMPO will assign a single point of contact to the receiving LEA.

7.2.26 HMPO's single point of contact will facilitate quarterly service reviews with the receiving LEA's nominated contacts where HMPO will provide evidence to support the SLAs within this document.

7.2.27 HMPO will provide support on working days 9am – 5pm UK local time, excluding public holidays. Outside of these hours a service desk will be available.

7.2.28 In the event of a serious data breach, the receiving LEA will notify HMPO in accordance with section 19 of the UDSA. The receiving LEA and HMPO will engage as appropriate to ensure that HMPO is effectively briefed on the data breach and the steps being taken by the receiving LEA to remedy/mitigate any such breach. Where appropriate such briefing may include HMPO (subject to reasonable and appropriate confidentiality undertakings) access to the receiving LEA's premises and records.

7.2.29 When carrying out any visit to the receiving LEA's premises or accessing records HMPO shall comply with any reasonable requirements of the receiving LEA in relation to health and safety and security and shall keep confidential all information disclosed to them by the receiving LEA.

Means of transfer of data/Information

7.3.1 Passport data is accessed via the DVA: Digital UI. DVA: Digital is a means by which Public Sector organisations can securely access passport data on a read-only basis via a web browser, no data is physically transferred or moved.

7.3.2 HMPO will create Organisation Administrator accounts for the receiving LEA's personnel as notified by the participant. The LEA Organisation Administrators are responsible for creating and maintaining Standard user accounts as needed under the terms of this PDSA.

7.3.3 The creation of a new user account will trigger DVA: Digital to auto email the user with a unique username and first-time password to enable each member of the receiving LEA's users to log on to the DVA: Digital System and activate their account.

Government Security Classification

7.4 The Government Security Classification for the data is OFFICIAL.

Who will have access to the shared personal data/designated points of contact

7.5 Access will only be permitted to the receiving LEA's authorised personnel and the Home Office who have:

I. the appropriate security clearance determined by HMPO to handle the data (the requirement is minimum CTC or above recognised by the UKSV) and
II. a genuine business need to access the information.

7.6 The receiving LEA must make provision for a single point of contact, to log queries and to deal with any faults on the Participant's system prior to referral to HMPO.

7.7 The receiving LEA will undertake regular reviews of their DVA: Digital user accounts and delete any accounts that are no longer required or are no longer appropriate, for example, where account holders are leaving, transferring to other roles, or where clearance lapses. Where the account is that of a user with an 'Organisation-Administrator' role the receiving LEA will notify HMPO who will administer deletion of the account.

7.8 The receiving LEA shall appoint users to act as DVA: Digital Organisation-Administrators. Organisation-Administrators have the ability to reset passwords, unlock accounts, create, amend, and delete accounts for standard users within their organisation.

7.9 The receiving LEA will appoint Primary contacts to be the single point of contact with HMPO. Any requests received from other members of the receiving LEA staff will be rejected by HMPO.

8 Lawful Data Protection Basis and Legal Power

Lawful basis for General Processing

8.1 The applicable lawful basis for processing personal data is outlined below for each Participant:

- HMPO's processing is: necessary for the performance of a task in the public interest, or for official functions, where the task or function has a basis in law
- The receiving LEA's processing is: necessary for the performance of a task in the public interest, or for official functions, where the task or function has a basis in law

8.2 As outlined in 'Schedule 1', Special Category personal data is being processed within the data sharing activity. The Participants acknowledge their individual responsibilities to comply with any applicable further special processing condition(s).

8.3 The Participants are not processing Criminal Offence/Criminal Conviction Data under this PDSA.

Legal Powers (for General Processing)

8.4 The applicable legal power(s) for each Participant's processing is outlined below:

- HMPOs legal power for this processing activity is: Common Law and Royal Prerogative

HMPO shares passport data with the receiving LEA under Common Law and Royal Prerogative.

- The receiving LEA's legal power for this processing activity is: Common Law

The Police derive their legal basis to share information, including personal data, from their Common Law Policing Purposes which include protecting life and property, preserving order, preventing the commission of offences, bringing offenders to justice.

Lawful Basis for Law Enforcement Processing

8.5 HMPO are not processing under Law Enforcement.

The receiving LEA confirm that processing of personal data for law enforcement purposes in the course of the activity described is 'necessary for the performance of a task carried out for law enforcement purposes by a competent authority.' For the purposes of this PDSA, the task carried out for law enforcement purposes is as follows under Schedule 8 of the Data Protection Act 2018 (conditions for sensitive processing under Part 3):

- Statutory etc purposes
- Administration of justice
- Protecting individual's vital interests
- Safeguarding of children and of individuals at risk
- Preventing fraud

8.6 The receiving LEA acknowledge their individual responsibility to have an Appropriate Policy Document in place where they are carrying out Sensitive Processing.

Legal Powers (for Law Enforcement processing)

8.7 The applicable legal power(s) for each Participant's processing is outlined below:

- HMPO are not processing under Law Enforcement.
- The receiving LEA's legal power for this processing activity is Common Law.

9 Third Party Processing

9.1 Neither participant will use a third party for processing personal data accessed as a result of this PDSA.

9.2 Where a Participant utilises a third-party Processer in the course of receiving personal data obtained from another Participant, they will:

- declare this to the sending Participant without undue delay;
- confirm the agreements required by UK Data Protection Legislation are in place with the third-party processer.

10 Onward Transmission

10.1 Participants in receipt of personal data from another Participant can onward transmit personal data where this sharing is in compliance with UK Data Protection Law and subject to any inherent restrictions.

10.2 In relation to Approved Data shared under this PDSA, the receiving LEA must send all onward disclosure requests to HMPO's intel hub via the following process:

10.3 Requests for onward disclosures that have not been pre-approved as part of this PDSA should be sent to S.31(1) supported by sufficient information to help HMPO determine if the proposed disclosure is consistent with UK Data Protection Legislation, human rights and other obligations. Requests should be e-mailed on the authorisation of a member of staff of the appropriate rank, including at least one further member of staff in the e-mail chain unless otherwise authorised to make direct requests.

10.4 The response to a request by HMPO may include a refusal to provide further information (where HMPO does not have the legal power to respond) or may include the provision of further data from HMPO records

10.5 HMPO will aim to provide the above support Monday to Friday between 9am and 5pm UK local time, excluding bank holidays. Queries will be resolved as quickly as possible. However, if an urgent response is required, please mark the subject line of your email with the word 'Urgent' and a response will be given within 24 hours. Where investigation is required, HMPO will work with the receiving LEA to determine the most appropriate course of action.

10.6 Outside the hours stated in section 10.5, onward disclosure is permitted between law enforcement agencies for Intel purposes, only where there is an Urgent operational requirement to do so. In such cases, prior authority should be sought by the appropriate rank (Inspector, SEO grade or equivalent). HMPO should be notified immediately that a disclosure has taken place, with an explanation of why the urgent disclosure was required. Notifications should be sent to S.31(1) and the e-mail titled "DVA Urgent Disclosure."

11 Transparency

Home Office

11.1 HMPO may share data with other government departments, law enforcement agencies and local authorities to help fulfil their aims and objectives.

Data sharing only takes place where there is a lawful power in place that permits the data sharing to occur.

A copy of HMPO Privacy Information Notice can be found here:
https://www.gov.uk/government/publications/hmpo-privacy-information-notice

The Receiving LEA

11.2 The receiving LEA's Privacy Notice that can be found on its internet site provides details of the purposes for which it processes personal data and provides necessary transparency and fairness. The sharing under this document is consistent with the details set out in the Privacy Notice. Exemptions/restrictions where permissible under the UK Data Protection Legislation may be applied. **www.northumbria.police.uk/hyg/fpnnorthum/privacy-notice/**

12 Retention

12.1 Participants accept that they must only store shared data in a form that identifies individuals for no longer than is necessary for the purposes for which they are processing the Personal Data in line with their retention procedures. Participants must have mechanisms in place to ensure appropriate retention and destruction of data.

Home Office

12.2 HMPO data is retained and destroyed in line with Home Office policies.

The Receiving LEA

12.3 Police data is retained and destroyed in line with the College of Policing's Authorised Professional Practice on Information Management and the NPCC's National Guidance on the minimum standards for the Retention and Disposal of Police Records

https://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/

13 Administration

13.1 The information sharing activity set out in this PDSA will involve regular sharing or access to personal data and will be subject to review as outlined in 13.2. This PDSA is effective from the date of the final Participant signature is documented.

13.2 This PDSA will be reviewed every 18 months, or whenever there is a significant change for any Participant that can impact the sharing arrangements outlined. Participants should engage with one another for an extraordinary review in circumstances including but not limited to:

- a change in the name or organisational structure of a participant;
- a change or extension of the purpose for processing;
- a change in the policies, procedures, methods, or protections surrounding the sharing activity;
- a change in the data protection law; or
- the identification or reporting of a security or privacy breach.

13.3 Reviews outside of the proposed review period can be called by representatives of either Participant.

13.4 A Process Specific Data Sharing Activity review should ensure the details documented within this PDSA including legal basis/powers/restrictions, contact details, purpose, expected benefits, process for sharing, data types, and all other surrounding procedures are accurate and factually correct.

13.5 Summary and version control above should contain high-level details of any reviews undertaken.

Costs

13.6 The provision of the Services to private sector and public sector customers is not cost-free to HMPO but involves capital outlay and continuing overhead costs. These costs will be passed on to the customer.

13.7 HMPO will charge the receiving LEA per licence for DVA: Digital UI browser access.

13.8 HMPO will charge the receiving LEA at the beginning of the financial year for the annual cost of all licences requested by the receiving LEA. Access will be granted once payment is received.

13.9 HMPO will not provide a refund if the receiving LEA reduces the number of licences that they hold during the financial year.

13.10 HMPO will charge the receiving LEA on a pro rata basis for additional licences. Part months will be charged at the full rate. Access will be granted once payment is received.

13.11 The charges will be reviewed by HMPO on an annual basis.

13.12 The receiving LEA will pay the Charges within 30 days of receipt of HMPO's invoice in respect of the same.

14 Termination

14.1 Participants may withdraw from the PDSA upon giving three months written notice to all Participants. A Participant who withdraws must continue to comply with the relevant terms of this PDSA in respect of any data that the Participant has obtained under those terms.

14.2 Termination notices must be referred to the signatories of the PDSA.

14.3 The Participants will have the right to terminate this PDSA should the following circumstances arise:

- a material breach by the other Participant of any of the terms of the UDSA.
- by reason of cost, resources or other factors beyond the control of either of the Participants.
- if any material change in circumstances occurs which, following negotiation between the Participants, in the reasonable opinion of either or all the Participants significantly impairs the value of the PDSA in meeting their objectives.

14.4 It is recognised that there may be circumstances where it may not be possible to terminate an information sharing activity such as set out in the situations below. Should such

circumstances arise, the Participants must refer to the signatories of this PDSA, or their successors, who will decide on how the information sharing activity will be managed.

- the sharing of information is essential to the Participants to provide their business service and termination of the PDSA would severely impact the organisation's ability to fulfil their statutory obligations and

- the sharing of information is to satisfy a legal requirement.

14.5 Where a decision is made to terminate this PDSA the Participants will mutually agree the procedure for the handling of any data/information shared under this PDSA.

15 Contacts

Business as Usual Contact Details:

Home Office	For queries, issues, or disputes regarding this Data Sharing Activity: S.31(1) Please refer to section 20 of the UDSA for Complaints/Issues/Disputes and Resolutions.
	For Review and Amendments to this PDSA: S.31(1)
	For Personal Data Breaches and Security Incidents: S.31(1) Please refer to section 19 of the UDSA for Personal Data Breaches and Security Incidents.
	For Freedom of Information Requests & EIR Requests: foirequests@homeoffice.gov.uk Please refer to section 17 of the UDSA for Freedom of Information & EIR Requests.
	For Data Subject Right Requests: DPA.Queries@hmpo.gov.uk Please refer to section 16 of the UDSA for Data Subject Right Requests
	For Finance Queries: S.31(1)

The Receiving LEA	For queries, issues, or disputes regarding this Data Sharing Activity: Operational Queries Resolution: S.31(1) Data Quality/Dispute Resolution: S.31(1) Please refer to section 20 of the UDSA for Complaints/Issues/Disputes and Resolutions.
	For Review and Amendments to this PDSA: S.31(1)
	For Personal Data Breaches and Security Incidents: S.31(1)

	Please refer to section 19 of the UDSA for Personal Data Breaches and Security Incidents.
	For Freedom of Information Requests & EIR Requests: Freedom.info@northumbria.police.uk Please refer to section 17 of the UDSA for Freedom of Information & EIR Requests.
	For Data Subject Right Requests: Data.protection@northumbria.police.uk Please refer to section 16 of the UDSA for Data Subject Right Requests.
	For Finance Queries: S.31(1)

Escalation Contact Details:

Home Office	For queries, issues, or disputes regarding this Data Sharing Activity: S.31(1) Please refer to section 20 of the UDSA for Complaints/Issues/Disputes and Resolutions.
	For Review and Amendments to this PDSA: S.31(1)
	For Personal Data Breaches and Security Incidents: S.31(1) Please refer to section 19 of the UDSA for Personal Data Breaches and Security Incidents.
	For Freedom of Information Requests & EIR Requests: S.31(1) Please refer to section 17 of the UDSA for Freedom of Information & EIR Requests.
	For Data Subject Right Requests: DPA.Queries@hmpo.gov.uk Please refer to section 16 of the UDSA for Data Subject Right Requests. For Finance Queries: S.31(1)

The Receiving LEA	For queries, issues, or disputes regarding this Data Sharing Activity: Operational Queries: S.31(1) [redacted] Data Quality/Dispute Resolution: S.31(1) [redacted] Please refer to section 20 of the UDSA for Complaints/Issues/Disputes and Resolutions.
	For Review and Amendments to this PDSA: Operational Queries: S.31(1) [redacted] Data Quality/Dispute Resolution: S.31(1) [redacted]
	For Personal Data Breaches and Security Incidents: S.31(1) [redacted] Please refer to section 19 of the UDSA for Personal Data Breaches and Security Incidents.
	For Freedom of Information Requests & EIR Requests: S.31(1) [redacted] Please refer to section 17 of the UDSA for Freedom of Information & EIR Requests.
	For Data Subject Right Requests: S.31(1) [redacted] Please refer to section 16 of the UDSA for Data Subject Right Requests.
	For Finance Queries: S.31(1) [redacted]

16 Signatories

Signed on behalf of the Home Office

I accept the terms of this Process-Specific Data Sharing Agreement on behalf of the HO:

Signature:	
Name:	
Position:	
Date:	

Signed on behalf of the Receiving LEA

I accept the terms of this Process-Specific Data Sharing Agreement on behalf of the Receiving LEA:

Signature:	
Name:	
Position:	
Date:	

Schedule 1 – Personal Data to be Shared

HM Passport Office

List of Data Items	Category of Data Personal Data/ Special Category Data/Sensitive Processing /Criminal Offence Data	Category of Data Subjects	Justification
• Passport number • Passport holder's first name • Passport holder's surname • Passport holder's date of birth • Passport issue date • Passport expiry date • Passport Imagery • Passport Application details, including associated addresses and telecommunications, Passport holder's parents' details, Countersignatory name, address and telecommunications (where available). HMPO will also return notification of whether or not the passport has been reported lost or stolen, and whether or not it appears on any of HMPO watch lists.	Personal Data submitted by applicant at the time of a passport application. Nationality may be inferred by existence of a passport record and is considered to be special category data by the Home Office. No criminal offence data will be processed.	UK Passport Holder Passport holder's parents' or grandparents' details, Countersignatory name,	Special Category data is processed lawfully by HMPO under Article 9(2)(g) UK GDPR and section 6(1)(b), Schedule 1 of the UK Data Protection Act 2018. Personal data is processed lawfully by HMPO under Article 6 (1) (e) of the United Kingdom General Data Protection Regulation (UK GDPR).

Northumbria Police – Force Intelligence Bureau (FIB)

List of Data Items	Category of Data Personal Data/ Special Category Data/Sensitive Processing /Criminal Offence Data	Category of Data Subjects	Justification
• Passport number • Passport holder's first name • Passport holder's surname • Passport holder's date of birth	Personal data is processed lawfully under Article 6(1)(c) or (d) or (e) UK GDPR Special Category Data Article 9(2)(c) or (g) UK GDPR And (including, but not limited to), the below paras of Schedule 1 of the DPA: •6. Statutory purposes •7. Administration of Justice •10. Preventing or detecting unlawful acts •11. Protecting the public against dishonesty etc •14. Preventing fraud •18. Safeguarding of children and individuals at risk No criminal offence data will be processed.	UK Passport Holder	Northumbria Police - Force Intelligence Bureau (FIB) requires DVA: Digital access for a Policing purpose to confirm suspect identity/Nationality and identify stolen/lost and fraudulent passports. DVA: Digital would be used in conjunction with E-Borders/Semaphore. Passport number is recorded against the flight manifest and linked to the person. Cases that give E-borders cause for concern are referred to Northumbria Force Intelligence for further investigation. E-Borders provide details that the passenger has checked in and provide flight details which include the passport number. The passport number will be searched on Semaphore which would display all the details. DVA: Digital would also be checked as the passport record would confirm all the details provided by the semaphore

			system. Details would then be referred to Northumbria Police - FIB if a criminal offence has occurred i.e. trafficking, child abduction, forced marriages. Serious category crimes. Northumbria Police - FIB would also conduct checks on DVA for investigations involving missing persons. Force Intelligence may also provide cover for Special Branch for National Security checks. The benefits of accessing DVA Digital are: • Identifying subjects and apprehension of offenders. • Conduct real time checks/24-7 access. • Do not have to rely on the Intel Hub Glasgow and wait for checks to be completed.