



Home Office



College of
Policing



Ministry
of Justice

OVEARCHING UMBRELLA DATA SHARING AGREEMENT (UDSA)

Between

THE SECRETARY OF STATE FOR THE HOME DEPARTMENT

And

**THE NATIONAL POLICE CHIEFS' COUNCIL (on behalf of Police Forces
of England & Wales)**

And

POLICE SERVICE OF SCOTLAND

And

POLICE SERVICE OF NORTHERN IRELAND

And

THE NATIONAL CRIME AGENCY

And

The COLLEGE OF POLICING

And

THE MINISTRY OF DEFENCE

And

THE SECRETARY OF STATE FOR JUSTICE

1. Summary and version control

Title	Overarching ‘Umbrella Data Sharing Agreement’ (UDSA) between Home Office, the National Police Chiefs’ Council, Police Service of Scotland, Police Service of Northern Ireland, National Crime Agency, College of Policing and the Ministry of Defence		
Author(s)	The parties involved in authoring this document were: • Home Office Data Sharing & Protocols Team • National Crime Agency Office of the Data Protection Officer • NPCC Police Freedom of Information and Data Protection Unit • Police Service of Scotland Information Assurance		
Next Review Date	June 2027		
Date Issued	July 2026		
Purpose	This overarching Umbrella Data Sharing Agreement (UDSA) sets out the high-level arrangements governing the sharing of information between the Participants to support the Participants to better deliver their respective business objectives and/or functions. This UDSA covers activities where the participants are acting independently as Controllers only; where the participants are Joint Controllers or the relationship is Controller to Processor a separate arrangement will be required.		
Contacts	Home Office: Datasharingand@homeoffice.gov.uk National Crime Agency (NCA): DPO@nca.gov.uk National Police Chiefs’ Council (NPCC): dpo@npcc.police.uk Police Scotland (PSoS): information.assurance@scotland.police.uk Police Service for Northern Ireland (PSNI): dataprotectionofficer@psni.police.uk College of Policing: data.protection@college.police.uk Ministry of Defence (MOD): ArmyPM-RMPEnquiriesMailbox@mod.gov.uk Ministry of Justice (MoJ): dataprotection@justice.gov.uk		
Disclosure	This document is suitable for publication and disclosure to organisations other than the participants.		
Retention Date	N/A while processing is ongoing		
Version control			
Version	Date	Summary of changes	Changes marked
V1.0	October 2019	Annual review	

V2.1	September 2020	Consultation and development of new version	New version incorporating all data sharing activity between parties
V2.2	October 2021	Annual Review	Yes. Addition of Police Services Northern Ireland to the Umbrella MoU
V2.3	April 2022	Final Annual Review	
V2.4	May 2023	Annual Review	
V3.0	December 2023	Final Annual Review	
V3.1	April 2024	Development of new version to include National Crime Agency.	Re-branded as Data Sharing Agreement; NCA and relevant legal power additions; specific UK GDPR/DPA references replaced with 'Data Protection legislation'; definitions updated; some Annexes replaced by schedules; sections re-arrange; summary page expanded; other language alterations and cross-referencing; addition of Annex B PDSA template guidance.
V3.2	May 2024	Consultation and amendments	Altered based on NPCC & HO feedback.
V3.3	June 2024	Consultation and amendments	Alterations based on PSoS and PSNI feedback.
V4.0	July 2024	Consultation, amendments, Signatures	Minor amendments and contact additions following NPCC Quality Assurance Panel. Signatures.
V4.1	December 2025	Consultation and amendments	Review & inclusion of College of Policing
V4.2	April 2026	Consultation and amendments	Review & inclusion of the Ministry of Defence
V4.3	July 2026	Consultation, amendments and signatures	Review & inclusion of Ministry of Justice following consultation with NPCC Quality Assurance Panel and signatures.

2. Contents

1. Summary and version control.....	2
2. Contents.....	4
3. Participants	5
4. Introduction	5
5. General principles	8
6. Aims and objectives of UDSA	9
7. Process-Specific data sharing agreement (PDSA) documents	9
8. Ad-hoc / proactive / one-off disclosures of information.....	10
9. Records of processing activities and data protection impact assessments.....	11
10. Controller status in respect of information sharing activities under this UDSA	12
11. Legal considerations	12
12. Fairness & transparency	13
13. Information handling, data accuracy and quality	14
14. Data security	14
15. Retention and destruction schedule	15
16. Data subject rights	15
17. Freedom of information / environmental information regulation requests.....	15
18. Onward disclosure of information to third parties	16
19. Personal data / information security breaches	17
20. Complaint resolution / issues, disputes and resolution between participants.....	17
21. Governance, monitoring and reviewing arrangements.....	18
22. Termination	18
23. Signatories	19
Schedule 1 - Participants	23
24. NPCC forces	23
25. Other police forces and law enforcement agencies, as separate signatories.....	24
26. National policing units and programmes	24
27. Home office departments	24
28. Ministry of Justice departments.....	25
Appendix A: TERMS AND DEFINITIONS.....	26

3. Participants

- 3.1 Collectively the organisations listed below will be referred to as the “**Participants**” and individually as a “**Participant**.”
- 3.2 A complete list of the Participants, including those represented by another signatory, is available in Schedule 1.
- 3.3 The signatories to this overarching Umbrella Data Sharing Agreement (UDSA) are:
- **THE SECRETARY OF STATE FOR THE HOME DEPARTMENT** of 2 Marsham Street, London, SW1P 4DF referred to as “**HO**” throughout this document
 - **NATIONAL POLICE CHIEFS’ COUNCIL** of 1st Floor, 50 Broadway London, SW1H 0BL, on behalf of the police forces of England & Wales as listed in Schedule 1, referred to as “**NPCC**”
 - **POLICE SERVICE OF SCOTLAND** of Tulliallan Castle, Kincardine, FK10 4BE, known as Police Scotland, referred to as “**PS**” throughout this document.
 - **POLICE SERVICES OF NORTHERN IRELAND** of Brooklyn House, 65 Knock Road, Belfast, County Antrim, BT5 6L, referred to as “**PSNI**” throughout this document.
 - **THE NATIONAL CRIME AGENCY** of Units 1-6 Citadel Place, Tinworth Street, London SE11 5EF, referred to as “**NCA**” throughout this document.
 - **THE COLLEGE OF POLICING** of Leamington Road, Ryton-on-Dunsmore, Coventry, Warwickshire, CV8 3EN, referred to as “**CoP**” throughout this document.
 - **THE MINISTRY OF DEFENCE (MOD)** of Whitehall, London SW1A 2HB comprises of the Ministry of Defence Police (MDP) and Ministry of Defence Service Police (MOD SP) forces - which includes: (i) the Royal Navy Police (ii) the Royal Military Police, (iii) the Royal Air Force Police (iv) the Defence Serious Crime Command.
 - **THE SECRETARY OF STATE FOR JUSTICE** of 102 Petty France, London, SW1H 9AJ referred to as “**MOJ**”

4. Introduction

- 4.1 The Participants recognise the importance of having clear guidelines to follow when sharing information to ensure the information is shared with appropriate safeguards and in accordance with the law.
- 4.2 This UDSA sets out the high-level arrangements that govern the sharing of information between the Participants. This UDSA supports the Participants in sharing information - to all or any other Participant(s) - where it will assist or benefit the delivery of their respective business objectives and/or functions. The objectives and functions of the Participants are outlined below (beginning at paragraph 4.9 below).
- 4.3 A key principle of this UDSA is that it is underpinned by a series of purpose-specific Process-Specific Data Sharing Agreements (PDSAs) that the Participants will arrange and sign for each purpose-specific information sharing activity entered into (see Process-Specific data sharing agreement (PDSA) documents). A template for these PDSAs is available as Annex A.
- 4.4 This UDSA is intended to be used for the sharing of Personal Data between Controllers. Where an information sharing activity is between the Participants acting collaboratively as Joint

Controllers, or where one of the Participants is a Processor, a separate agreement will need to be put in place.

- 4.5 As information sharing is a reciprocal arrangement between the Participants, the requirements contained in this UDSA shall equally apply to all Participants unless otherwise specified.
- 4.6 This UDSA 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.
- 4.7 This UDSA has been written with due consideration of the contents of the updated statutory Data Sharing Code of Practice (2021) issued by the Information Commissioner's Office (ICO).
- 4.8 As such, the participants are committed to working in partnership for the purposes of supporting and delivering their respective business functions as set out below:

Role of HO:

- 4.9 HO is the lead government department for immigration and passports, drugs policy, crime, fire, counter-terrorism and police.
- 4.10 This is a link to the [HO](#) website, which provides more information on the role of the HO. The roles and functions of HO can be non-exhaustively summarised as covering:
 - working on the problems caused by illegal drug use;
 - shaping the alcohol strategy, policy and licensing conditions;
 - keeping the United Kingdom safe from the threat of terrorism;
 - reducing and preventing crime, and ensuring people feel safe in their homes and communities;
 - securing the UK border and controlling immigration;
 - considering applications to enter and stay in the UK;
 - issuing passports and visas;
 - supporting visible, responsible and accountable policing by empowering the public and freeing up the police to fight crime; and
 - fire prevention and rescue.

Role of NPCC, PS and PSNI:

- 4.11 The NPCC brings Police forces in the UK together to help policing coordinate operations, reform, improve and provide value for money. This is a link to the [NPCC](#) website, which provides more information on the role of NPCC.
- 4.12 PS was formally established on 1 April 2013 and is responsible for policing across the length and breadth of Scotland. PS's purpose is to improve the safety and wellbeing of people, places and communities in Scotland.
- 4.13 PSNI was formally established on 4th November 2001 and is responsible for policing across all of Northern Ireland. PSNI purpose is to keep people safe through preventing crime, detecting offenders and protecting the most vulnerable in our society.

4.14 NPCC, PS, and PSNI functions can be non-exhaustively summarised as covering:

- Protection of life and property;
- prevention and detection of crime;
- preservation of order;
- prevention of the commission of offences;
- the bringing of offenders to justice; and
- additional duties that are prescribed under legislation and common law.

Role of the NCA

4.15 The NCA has the following functions, which are set out in greater detail in s.1 of the Crime and Courts Act 2013 (CCA):

- Combating organised and serious crime, through prevention, detection and investigation;
- Securing that activities to combat organised and serious crime are undertaken by both the NCA and others, including by improving co-operation between those who carry out such activities and improving the coordination of such activities;
- Undertaking activities to reduce organised and serious crime in other ways and to mitigate its consequences;
- Gathering, storing, processing, analysing and disseminating information relevant to combating crime; and
- Tackling criminal finances, pursuant to the Proceeds of Crime Act 2002.

Role of the CoP

4.16 The College of Policing (CoP) is the professional body for policing in England and Wales. It is responsible for setting standards in professional development, accrediting training providers, and supporting the continuous professional development of police officers and staff. The College aims to ensure that policing is based on the best available evidence and promotes the highest standards of integrity and professionalism.

Role of the MOD

4.17 The MOD oversees an interconnected policing capability that integrates civilian law enforcement with military policing capabilities, ensuring comprehensive security across the Defence estate. Directly beneath this organisational authority sits:

- **MDP.** The MDP was formally established on 1 October 1971, and its modern legal framework is set out in the Ministry of Defence Police Act 1987. The MDP as a national civilian police force, protects Defence people, property, information, and nuclear assets through armed policing, security operations, and specialist investigations. The MDP is listed as a NPCC force in Schedule 1.

- **MOD SP.** The MOD SP by virtue of the Armed Forces Act 2006 (AFA 2006), provide the primary investigative capability to deal with both Service Disciplinary Offences and Criminal Conduct Offences involving Persons Subject to Service Law (PSSL) and Civilians Subject to Service Discipline (CSSD). The role of the MOD SP is to support operational effectiveness and wider military capability in the UK and overseas, in both hostile and benign environments, by contributing to the:
 - Prevention and detection of crime by persons subject to Service Discipline contrary to the AFA 2006;
 - Maintenance and enforcement of Service discipline and good order;
 - Protection and safe deployment of Service personnel and assets.

Role of MOJ

- 4.18 The MOJ is a major government department at the heart of the justice system, working to protect and advance the principles of justice with a vision to deliver a world-class justice system that works for everyone in society. Further information can be found on the UK government website [here](#).
- 4.19 The MOJ's responsibility for the justice system includes:
- Courts
 - Prisons
 - Probation services
 - Attendance centres

5. General principles

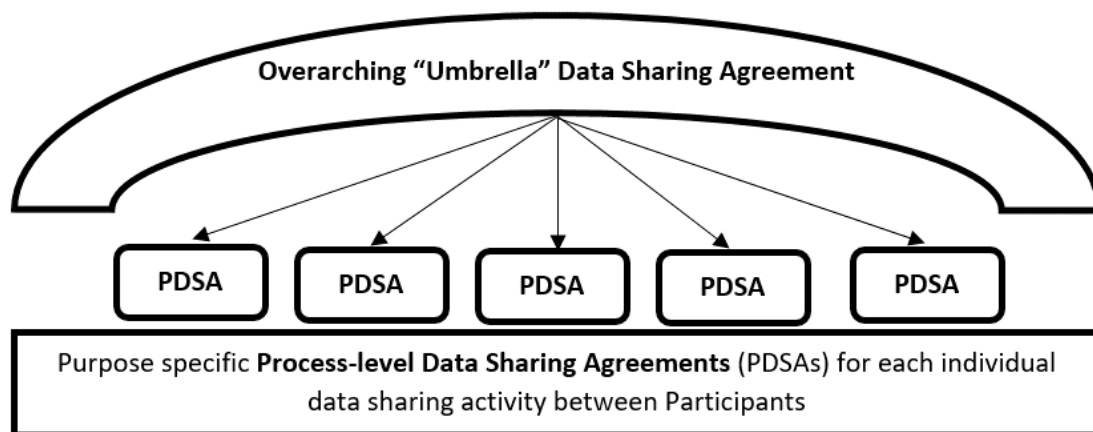
- 5.1 **Co-operation:** The Participants will cooperate in good faith to fulfil the purpose of this UDSA and any purpose-specific information sharing documents made under it.
- 5.2 **UK Data Protection Legislation:** The Participants will comply with the requirements of the UK Data Protection Legislation.
- 5.3 **The Participants (with the exception of CoP) are Competent Authorities** as specified in Schedule 7 of the DPA. As such, this UDSA has been created to support the exchange of information between the Participants for General and/or Law Enforcement Purposes depending on the nature and purpose of the sharing activity. It is incumbent on all Participants to recognise that any information shared must be justified on the merits of each case.
- 5.4 **Human Rights Legislation:** The Participants will comply with the requirement of the Human Rights Act 1998 and where relevant the Common Law Duty of Confidentiality and other relevant legislation.
- 5.5 **Data Security Standards:** The Participants will only share data in accordance with the relevant standards for data quality and security as set out in sections 13 and 14 of this UDSA.
- 5.6 **Process-Specific Data Sharing Agreements (PDSAs):** The Participants will write PDSAs for any purpose-specific information sharing activities entered into under this UDSA. PDSAs can be created for use between any, or all, of the Participants; there is no requirement for all Participants of the UDSA to be involved in all activities described within purpose specific PDSAs.

- 5.7 **Necessary and Proportionate:** Participants will ensure that any data shared under this UDSA or associated PDSAs is adequate, relevant, and not excessive in relation to the purpose or purposes for which they are being shared.

6. Aims and objectives of UDSA

- 6.1 Organisations that share personal data have a legal responsibility to ensure that the disclosure of information is both lawful and subject to adequate controls. This UDSA aims to:

- provide a formal record of high-level commitment and agreement between Participants
 - provide an overarching framework that the underpinning purpose-specific PDSAs must follow (see diagram below)
- set out the high-level principles that will govern the sharing of information between the Participants including the onward disclosure of personal data to third parties (see Onward disclosure of information to third parties)
 - describe the data security procedures necessary to ensure compliance with the UK Data Protection Legislation and any other specific security requirements
 - describe the process for managing unauthorised disclosures or loss or damage to information; and,
 - describe the process for monitoring and reviewing the use of this UDSA.



7. Process-Specific data sharing agreement (PDSA) documents

- 7.1 PDSAs will be used to manage any purpose-specific information sharing activities entered into by the Participants and will provide the detail specifically related to that information sharing activity. These documents will be subject to the arrangements within this UDSA and must reference this UDSA.
- 7.2 The PDSA document is designed for information sharing activities where the Participants are acting as Controllers as defined in Data Protection Legislation.
- 7.3 A PDSA template has been produced to encourage consistency. This template is available at Annex A; guidance on how to complete a PDSA is available at Annex B. Use of the PDSA template is recommended; however, another template can be used only where it follows the parameters laid out in this UDSA, including a minimum of the following details:

- the Participants involved in the information sharing activity
- the purpose and benefits of the information sharing activity
- type of information sharing activity (one-off/routine/regular)
- the legal powers permitting the sharing of data
- the lawful bases for the data sharing
- scope of data to be shared
- the process and method of information sharing
- onward disclosures to third parties
- monitoring and reviewing arrangements
- termination procedures
- designated points of contacts for data subject rights, Freedom of Information requests (Fol), Environment Information Requests (EIR), reporting personal data breaches, and reporting information security incidents
- signatories to the PDSA

7.4 The circumstances and the type of data sharing activities for which Participants will consider putting in place a PDSA are set out below:

- **Frequency & Scale:** When entering a regular or large-scale information sharing activity with all or some of the other Participant(s).
- **Direct System Access:** When providing direct access to data systems owned by any Participant.
- **Sensitive Data:** When sharing sensitive/special category and/or criminal conviction offence data.
- **Profile & Political Sensitivity:** When the data sharing activity itself is high profile and/or politically sensitive.
- **Governance:** When any of the Participants' governance process requires a written document for the data sharing activity.
- **Data Protection Impact Assessment (DPIA):** When the outcome of a DPIA requires a written purpose-specific data sharing document for the data sharing activity.

8. Ad-hoc / proactive / one-off disclosures of information

8.1 Aside from the purpose-specific information sharing activities as described above in Process-Specific data sharing agreement (PDSA) documents, the Participants may in some circumstances decide to share or be asked to share personal data by the other Participant(s) for an urgent or compelling situation or as an ad-hoc/one-off disclosure that may fall outside of any routine information sharing arrangements. These disclosures can take place under this UDSA (without a supporting PDSA), as long the disclosure is necessary and proportionate, and complies with UK Data Protection Legislation and the principles detailed in this UDSA.

- 8.2 Proactive disclosures of information can also take place between Participants under this UDSA (without a supporting PDSA) for any of their respective statutory functions where there is a lawful basis to do so. Many of these disclosures will be spontaneous and will cover a range of each Participants' functions.
- 8.3 Where the Participants are required to make disclosures of data derived from the other Participant for a court order or where there is an overriding requirement for disclosure in the public interest, these disclosures can take place without the need to consult with the Participant(s) who is/are the source of the data.
- 8.4 The above disclosures will not need to be subject to an additional PDSA.
- 8.5 When considering an ad-hoc/one-off/proactive disclosure of information the Participants will also follow their internal decision-making models in respect of the disclosure and record keeping. Ad hoc data requests, and records of them, should include the following information as a minimum:
- Details of requesting Participant
 - Date of request
 - Date(s) by which provision of data is required
 - Role of person requesting data
 - Whether your local Data Protection Officer or equivalent governance teams have been consulted
 - Description of data requested
 - Purpose of request
 - Whether there will be specific arrangements for retention / deletion of any data shared
 - Any circumstances of the proposed sharing that could result in a risk to the data subjects or other individuals
 - Means of transfer (must be by secure)

9. Records of processing activities and data protection impact assessments

Record of Processing Activities (RoPA)

- 9.1 The Participants will maintain a record of information sharing activities entered into pursuant to this UDSA in compliance with the requirements of UK Data Protection Law.
- 9.2 The record will include the following as a minimum:
- details of the Participants who are involved in the information sharing activity
 - the purpose of the information sharing activity
 - the lawful basis for the information sharing activity

- categories of personal data shared and categories of data subject the personal data relates to
- the retention schedules
- the date the information sharing document was signed by the Participants and the agreed review date.

Data Protection Impact Assessments (DPIAs)

- 9.3 The Participants will ensure before any information sharing takes place under this UDSA, or associated PDSA(s), that the completion of a DPIA is considered when required by UK Data Protection Law.
- 9.4 The Participants will confirm in their relevant PDSA whether a DPIA or threshold/screening assessment was carried out.

10. Controller status in respect of information sharing activities under this UDSA

- 10.1 The Participants accept that this UDSA only covers sharing of information between Participants as Controllers.
- 10.2 Where Participants wish to enter into Joint Controller or Controller to Processor relationships with each other a separate arrangement will be required.

11. Legal considerations

- 11.1 This UDSA is not intended to be legally binding. It does not create a lawful means for the exchange of information; but rather documents a framework of the information sharing processes and procedures between Participants.
- 11.2 In signing to this UDSA; the Participants accept that sharing of personal data and/or special category data personal data and/or criminal offence data will only occur where:
- they have a legal power to share
 - the sharing is not in contravention of any rule of law, including the Common Law Duty of Confidentiality and Human Rights Act 1998
 - the sharing is compliant with the UK Data Protection Legislation.

Legal Powers

- 11.3 As a ministerial government department, the HO's legal power to share data may be set out expressly in statute, implied from statutory powers and functions, or derived from Common Law. In the majority of cases, the HO relies on Common Law as its legal power to share personal data. Where a statutory power to share certain data is in place, though, the statutory power will take precedence, effectively limiting the application of common law to scenarios other than those covered by statutory provisions.
- 11.4 The Police forces represented by the NPCC, PS and PSNI derive their power to share personal data from their Common Law Policing Purposes, the statutory Code of Practice on the Police Information and Records Management (PIRM) 2023 still referenced 'locally' as the Management of Police Information (MoPI) and may also rely on other statute. The latter

include express statutory obligations to share and express statutory powers, or implied statutory powers to do so.

- 11.5 The Participants acknowledge the statutory power for the NCA to share and receive data relating to its functions pursuant to this UDSA, and associated PDSAs, deriving from S7 of the CCA 2013, subject to schedule 7 to the CCA 2013. The use of the information sharing gateway under section 7 of the CCA 2013 by the Participants will be subject to the statutory restrictions set out in schedule 7 to the CCA 2013. In particular, the Participants recognise section 7 will not authorise a disclosure of Personal Data in contravention of Data Protection Legislation. The Participants acknowledge that the NCA is permitted under section 7(3) of the CCA to use information obtained under this UDSA, and associates PDSAs, in connection with any other NCA function and is permitted under section 7(4) of the CCA to disclose information onwards if it is for any permitted purpose.
- 11.6 The Participants acknowledge the statutory power for the MOD SP to share and receive information relating to its functions pursuant to this UDSA and associated PDSAs deriving from the AFA 2006. In addition, as a Crown body, the MOD relies on its prerogative powers that emanate from Common Law.
- 11.7 As a ministerial government department, the MOJ's legal power to share data may be set out expressly in statute, implied from statutory powers and functions, or derived from Common Law.
- 11.8 When relying on a legal power to share information the Participants must set out the specific legal power that permits the disclosing, receiving, and/or further processing of personal data in the relevant PDSA for the information sharing activity.
- 11.9 The Participants note that NPCC, PS, PSNI, HO, CoP MOD, and MOJ are public authorities for the purposes of UK Data Protection Legislation. The Participants note that the NCA is not a public authority for the purposes UK Data Protection Legislation.

12. Fairness & transparency

- 12.1 The Participants must ensure that they comply with their obligations under the lawfulness, fairness and transparency requirements as set out in the first data protection principle. Participants are responsible for:
- recognising that the public have rights of privacy and confidentiality and that sharing and other processing of person identifiable information will respect these rights
 - ensuring that the public are informed of the purposes for processing/sharing their information through an appropriate privacy notice, unless there is a legal obligation or DPA exemption that overrides this requirement
 - the public are informed which other organisations its data may be disclosed to and consideration is given to whether consent of the data subject is required, and if so, will be sought (and complied with), unless there is a legal obligation or DPA exemption that overrides this requirement.
 - NB: It should be noted that the transparency requirement differs when processing for law enforcement processing.
- 12.2 The Participants will confirm in their relevant PDSA how the information sharing activity satisfies the above requirements.

13. Information handling, data accuracy and quality

- 13.1 The Participants will make reasonable endeavours to ensure that the data being shared is checked before disclosure for accuracy and relevance in accordance with the accuracy requirements as set out in the fourth data protection principle. All Participants will ensure data integrity meets their standards.
- 13.2 Each PDSA to this UDSA will specify the means by which the information will be shared, handled and stored for each purpose-specific information sharing activity entered into, and outline how the information sharing activity will comply with the data quality principles of data minimisation and accuracy.
- 13.3 In the event that a Participant becomes aware of any inaccuracy, requirement to delete/erase, or other defect in information that has been shared it will notify any other Participants that have received or shared the information.
- 13.4 Where anonymised data, pseudonymised data or non-personal data is shared, the recipient of that information will not attempt to re-identify any individual by analysing or combining it with other information without prior written agreement of the sending Participant, taking into account the relevant provisions of the Data Protection Legislation.

14. Data security

- 14.1 Each PDSA should outline how the information sharing activity will comply with the integrity and confidentiality principle and also include the following information handling and data security standards:
- **Portable Storage:** Information should not be transferred or stored on any type of portable device unless absolutely necessary, and if so, it must be encrypted, and password protected to an agreed standard.
 - **Encryption:** Information should not be transferred by email or other form of electronic communication unless adequate security measures are in place to preserve the security and confidentiality of that information, e.g. secure encrypted emails, end to end, with secure data storage.
 - **Policies and Procedures:** The Participants will have in place policies and procedures governing the secure storage of information for both electronic and manual systems.
 - **Knowledge and Awareness:** The Participants will take steps to ensure that all staff are adequately trained and are aware of their responsibilities under UK Data Protection Legislation and this UDSA.
 - **Access Controls:** Access to information received by the Participants pursuant to this UDSA or associated PDSAs must be restricted to employees on a legitimate need-to-know basis, and with security clearance at the appropriate level.
 - **Security Classification:** The Participants will comply with the Government Security Classifications Policy ([Government Security Classification Policy](#)) and Government HMG Security Policy Framework Security Policy Framework where applicable.
 - **HMG Security Policy Framework (HMG SPF):** The Participants must process the data being shared in compliance with HM Government Security Policy Framework (HMG SPF) guidance issued by the Cabinet Office: HMG SPF guidance document can be accessed via the following link [Security Policy Framework](#)

15. Retention and destruction schedule

- 15.1 Participants will outline how the information sharing activity will comply with the storage limitation principle in the relevant PDSA and undertake to store information being shared securely with access restricted to authorised personnel only.
- 15.2 Participants will have documented policies on the retention and destruction of shared information.
- 15.3 Participants will not keep information longer than necessary for the agreed purpose set out in the relevant PDSA.
- 15.4 Where specific information sharing activities are entered into by the Participants; the approach to retention should be decided at the outset prior to commencing the information sharing activity and set out in the respective PDSA for that information sharing activity.
- 15.5 Where a PDSA has been terminated, the Participants will follow any procedure set out in that PDSA in relation to the handling of the data previously processed under the terminated PDSA.

16. Data subject rights

- 16.1 Under UK Data Protection Legislation, data subject rights vary according to the data protection regime relied upon to share the personal data.
- 16.2 In the event a request to exercise a particular right is received from a data subject under this UDSA or any associated PDSAs, the Participants will respond to the request in accordance with the requirements of the UK Data Protection Legislation.
- 16.3 Individuals can request a copy of all the information that either Participant holds on them, by making a Right of Access Request (RAR). This may include information that was disclosed to that Participant under this UDSA or any associated PDSAs. Where this is the case, as a matter of good practice, the Participants will liaise with each other if appropriate to identify whether the release of the information to the individual will not prejudice any ongoing investigation/proceedings.
- 16.4 Information provided to data subjects may be restricted where it is necessary and proportionate to do so in accordance with UK Data Protection Law.
- 16.5 Where a data subject rights request, court order, or other mechanism results in a requirement to rectify, erase, or otherwise restrict any personal data shared under this UDSA, or any associated PDSAs, Participants will inform any other Participants who have received or shared the data of the existence, details, and action taken related to this rectification/erasure/restriction requirement.
- 16.6 Contact details for responding to data subject right requests will be provided in the relevant PDSA for that information sharing activity.

17. Freedom of information / environmental information regulation requests

- 17.1 HO, MOD, MOJ, NPCC and all Police Forces in England and Wales and Northern Ireland are public authorities for the purposes of the Freedom of Information Act 2000 (or "FOIA") and for the purposes of the Environmental Information Regulations 2004 (EIR). This legislation covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland.

- 17.2 The NCA is not a public authority for the purposes of the Freedom of Information Act 2000 ("FOIA"). The NCA will not disclose any information in response to a FOIA request. Furthermore, information provided by or relating to the NCA is absolutely exempt from disclosure under section 23 FOIA.
- 17.3 Information held by Scottish public authorities is covered by Scotland's own Freedom of Information (Scotland) Act 2002 and environmental information held by Scottish public authorities is covered by the Environmental Information (Scotland) Regulations 2004.
- 17.4 The Participants will demonstrate a commitment to openness and transparency regarding information sharing activities. In the event that a FOI/EIR request relating to information sharing activities under this UDSA or any associated PDSA is received by either Participant, each Participant agrees to:
- consult with the other Participant(s) on whether or not to disclose any information obtained from that Participant
 - as a matter of good practice, the receiving Participant will liaise with the originating Participant to ensure that the release of the information to the individual will not prejudice any ongoing investigation/proceedings and will apply any appropriate exemptions to prevent disclosure where necessary
 - allow the other Participant a period of at least 5 working days to respond to that consultation
 - consider any arguments from the other Participant as to why the data should not be disclosed, and where possible reach agreement before any disclosure is made.
- 17.5 Contact details for processing FOI/EIR requests will be provided in the relevant PDSA for that information sharing activity.
- 17.6 It is noted that, ultimately, the decision to disclose requested information or apply exemptions lies with the Participant who received the request.

18. Onward disclosure of information to third parties

- 18.1 Any personal data shared as a result of this UDSA (and any associated PDSAs) which is then retained by the receiving Participant(s); the receiving Participant(s) will become Controllers of that data and will adopt the associated Data Protection obligations.
- 18.2 As Controller for the data, the receiving Participant can onwardly disclose the data to third-parties subject to any inherent legal restrictions that may apply to the data. These restrictions may include but are not limited to:
- specific statutory prohibitions on further sharing
 - copyright restrictions
 - a duty of confidence that might affect your ability to onwardly share the data.
- 18.3 The Participants note that information provided by the NCA is subject to the onward sharing restrictions in [Schedule 7 of the CCA](#) which prohibits the disclosure of any data received from the NCA except with consent of the NCA. Any such consent will be given in writing and not unreasonably withheld.

- 18.4 Where a purpose-specific information sharing activity is entered into, the relevant PDSA will articulate the arrangements where routine onward disclosures are intended to ensure that they take place in accordance with the Data Protection Legislation.
- 18.5 Where applicable the relevant PDSA will state whether there are any restrictions on the Participants ability to onwardly share the data with third parties.
- 18.6 Where the receiving Participant wishes to make an onward disclosure of data that is subject to a restriction as set out in paragraph 18.2 above, the receiving Participant must consider whether it is necessary to consult with the originator of the information before any disclosure is made giving the reasons for this disclosure including the justification and lawful basis, and where applicable decide specific arrangements in the relevant PDSAs to manage any associated risks.
- 18.7 Participants will not make any public statement or press release about this UDSA without the express consent of the other Participant(s).
- 18.8 The Participants will not transfer Personal Data supplied under this UDSA nor any associated PDSAs to a country or territory outside of the UK, save as in accordance with the terms of this UDSA, any relevant PDSAs, and UK Data Protection Legislation.

19. Personal data / information security breaches

- 19.1 It is the responsibility of all Participants to comply with the obligations laid out in UK Data Protection Law in the event of personal data breach.
- 19.2 Where it becomes apparent that a personal data breach or information security incident has occurred that is **not covered by** a supporting PDSA, the matter must be dealt with in accordance with the relevant Participant's procedures. In addition, other relevant Participants should be informed of the breach / incident within a reasonable timeframe post discovery. Participant contact details for this purpose are as follows: can be found in the Summary and version control page of this UDSA.
- 19.3 Where it becomes apparent that a personal data breach or information security incident has occurred involving information sharing that is **covered by** a supporting PDSA, the matter must be dealt with in accordance with the procedures set out in that PDSA.
- 19.4 The designated points of contact will discuss and jointly decide the next steps relating to the incident, taking specialist advice where appropriate. Such arrangements will include (but will not be limited to) containment of the incident and mitigation of any ongoing risk, recovery of the personal data, and assessing whether the Information Commissioner and/or the data subjects will be notified. The arrangements may vary in each case, depending on the sensitivity of the personal data and the nature of the loss or unauthorised disclosure. Where appropriate, and if relevant to the incident, disciplinary misconduct action and/or criminal proceedings may be considered.

20. Complaint resolution / issues, disputes and resolution between participants

Complaint Resolution Procedure

- 20.1 Complaints about the use of shared information in relation to this UDSA and any associated PDSAs should be dealt with under the relevant complaints' procedure of the Participant whose actions are subject of the complaint.

- 20.2 Participants accept to co-operate with each other in the investigation of any complaint or other investigation about the use of the information shared.
- 20.3 The outcome/resolution of any complaint will be notified to the other Participants to this UDSA.

Issues, Disputes and Resolution between Participants Procedure

- 20.4 Any issues or disputes that arise as a result of data sharing activities covered by this UDSA must be directed to the relevant contact points listed in the relevant PDSA. Each Participant will be responsible for escalating the issue as necessary within their given organisations.
- 20.5 Should the problem be of an urgent nature; it must be reported in writing within 24 hours of the problem occurring to the designated points of contact listed in the relevant PDSA.

21. Governance, monitoring and reviewing arrangements

Date UDSA comes into effect

- 21.1 This UDSA comes into effect on the date it is signed by the Participants.

Governance

- 21.2 The HO Data Sharing Protocols Team DataSharing@homeoffice.gov.uk will be responsible for prompting the review of this UDSA.
- 21.3 Each PDSA will include the named points of contact for responsible for the review of the PDSA for any specific information sharing activities entered into.

Review Process of UDSA

- 21.4 The UDSA will run indefinitely but must be reviewed at least every three years to consider whether the UDSA is still necessary and fit for purpose.
- 21.5 Reviews outside of the approved schedule can be called by representatives of either Participant for example where new or revised legislation or cross-government guidance necessitates an earlier review. All Participants accept to cooperate fully in such reviews.
- 21.6 Reviews for individual process specific data sharing agreements (PDSAs) will be outlined within the related PDSA and will differ to the review period for the UDSA.

22. Termination

UDSA

- 22.1 This UDSA will remain in effect unless terminated by any of the Participants. Any of the Participants may terminate this UDSA by giving three months' written notice to the other Participant(s) in the following circumstances:
- By reason of cost, resources or other factors beyond the control of the Participants;
 - If any material change occurs which, in the opinion of a Participant, and following negotiation, significantly impairs the value of the UDSA in meeting its objectives.
 - In the event of serious breach of the terms of this UDSA.
- 22.2 The termination notices will be referred to the signatories of the UDSA.

22.3 In the event of termination of this UDSA; any PDSAs made under it must be reviewed in accordance with the termination provisions contained in the relevant PDSAs.

PDSAs

22.4 The termination provisions for any purpose-specific information sharing activities will be set out in the relevant PDSA for that information sharing activity.

22.5 Termination notices must be referred to the signatories of the PDSA and the UDSA in the following circumstances as a minimum:

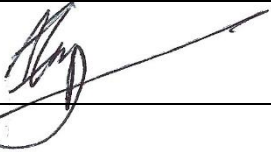
- where the sharing of information under the PDSA is essential to the Participants to provide their business service and/or
- where the sharing of information under the PDSA is to satisfy a legal requirement and termination of the PDSA would severely impact the organisation's ability to fulfil their legal obligations.

22.6 The signatories will consult with each other and decide on the next steps to take to ensure business continuity/legal obligations continue to be met and to consult on the handling of any information shared.

23. Signatories

Signed on behalf of the Home Office (HO)

23.1 I accept the terms of the overarching Umbrella Data Sharing Agreement on behalf of the HO:

Signature:	
Name:	Andy Gregory
Position:	Deputy Director, Data Services & Analytics, HO DDaT
Date:	03/08/2026

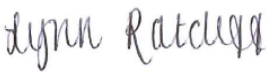
Signed on behalf of National Police Chiefs' Council (NPCC)

23.2 I accept the terms of the overarching Umbrella Data Sharing Agreement on behalf of NPCC:

Signature:	
Name:	Chief Constable C.J. Todd
Position:	Chair National Data & Analytics Board, NPCC Data Analytics Lead
Date:	12/08/2026

Signed on behalf of Police Service of Scotland (PS)

23.3 I accept the terms of the overarching Umbrella Data Sharing Agreement on behalf of PS:

Signature:	
Name:	Lynn Ratcliff
Position:	Assistant Chief Constable
Date:	21/08/2026

Signed on behalf of Police Service of Northern Ireland (PSNI)

23.4 I accept the terms of the overarching Umbrella Data Sharing Agreement on behalf of PSNI:

Signature	
Name	Bobby Singleton
Position	Deputy Chief Constable and Senior Information Risk Owner
Date	14/09/2026

Signed on behalf of National Crime Agency

23.5 I accept the terms of the overarching Umbrella Data Sharing Agreement on behalf of NCA:

Signature	
Name	Robert Jones CBE
Position	Director General (Operations)
Date	07/09/2026

Signed on behalf of the College of Policing

23.6 I accept the terms of the overarching Umbrella Data Sharing Agreement on behalf of CoP:

Signature	
Name	Luke Edwards
Position	SIRO, Chief Finance Officer & Director of Delivery
Date	28/08/2026

Signed on behalf of the MOD Service Police Forces:

23.7 The following MOD signatories accept the terms of the overarching Umbrella Data Sharing Agreement on behalf of the MOD:

Signature	
Name	Commander Ronni McClaren
Position	Provost Marshal (Royal Navy)
Date	13/08/2026

Signature	
Name	Brigadier David Dray MBE
Position	Provost Marshal (Army)
Date	06/08/2026

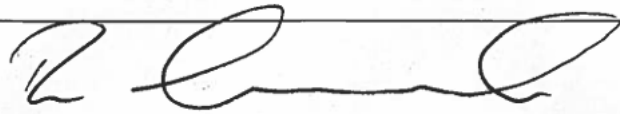
Signature	
Name	Group Captain Samantha Bunn
Position	Provost Marshal (RAF)
Date	04/08/2026

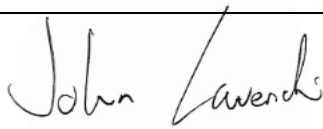
Signature	<i>K Rotchell</i>
Name	Brigadier Kris Rotchell
Position	Provost Marshal (Serious Crime)
Date	13/08/2026

Signed on behalf of the Ministry of Justice

23.8 I accept the terms of the overarching Umbrella Data Sharing Agreement on behalf of MOJ:

Signature	
Name	Hugh Stickland
Position	Chief Data Officer, Chief Scientific Adviser, MOJ HQ
Date	08/08/2026

Signature	
Name	Ben Charnock
Position	Executive Director Strategy, Performance & Standards, HMPPS
Date	06/08/2026

Signature	
Name	John Laverick
Position	Chief Digital Information Officer & Senior Information Risk Owner, HMCTS
Date	10/08/2026

Schedule 1 - Participants

24. NPCC forces

The Chief Officers of the Police Forces listed below are Participants to this agreement as represented by the NPCC. It is acknowledged that each Chief Constable is Controller under UK Data Protection Legislation for the processing of Personal Data by their Force and activity under this agreement is undertaken within parameters of the NPCC Joint Controllership Agreement.

Avon & Somerset Constabulary	Lincolnshire Police
Bedfordshire Police	Merseyside Police
British Transport Police	Metropolitan Police Service
Cambridgeshire Constabulary	Ministry of Defence Police
Cheshire Constabulary	Norfolk Constabulary
City of London Police	North Wales Police
Civil Nuclear Constabulary	North Yorkshire Police
Cleveland Police	Northamptonshire Police
Cumbria Constabulary	Northumbria Police
Derbyshire Constabulary	Nottinghamshire Police
Devon & Cornwall Police	South Wales Police
Dorset Police	South Yorkshire Police
Durham Constabulary	Staffordshire Police
Dyfed-Powys Police	Suffolk Constabulary
Essex Police	Surrey Police
Gloucestershire Constabulary	Sussex Police
Greater Manchester Police	Thames Valley Police
Gwent Police	Warwickshire Police
Hampshire & Isle of Wight Constabulary	West Mercia Police
Hertfordshire Constabulary	West Midlands Police
Humberside Police	West Yorkshire Police
Kent Police	Wiltshire Police
Lancashire Constabulary	
Leicestershire Constabulary	

25. Other police forces and law enforcement agencies, as separate signatories

25.1 Police Service of Scotland, known as Police Scotland (PS)

25.2 Police Service of Northern Ireland (PSNI)

25.3 The National Crime Agency (NCA)

25.4 The College of Policing (CoP)

25.5 The MOD SP – Royal Navy Police, Royal Military Police, Royal Air Force Police and Defence Serious Crime Command.

26. National policing units and programmes

26.1 It is acknowledged that UK police forces will often work collaboratively as a police service within national policing units or under national programmes of work. It is expected that data sharing activity as part of this type of national work could be supported using this UDSA and PDSA process. Examples of national policing units and programmes are:

- Counter Terrorism Policing (CTP) is a collaboration of UK police forces working with the UK intelligence community to help protect the public and our national security by preventing, deterring and investigating terrorist activity.
- The National Police Coordination Centre (NPoCC) provides support to forces across the United Kingdom, Crown Dependencies and British Overseas Territories. It is made up of a small number of officers and staff drawn on secondment from police forces across the UK, formed into two teams (Operations, and Strategic Intelligence and Briefing), which is funded by contributions from all forces.
- The Police Race Action Plan is the biggest coordinated effort ever across every police force in England & Wales to improve trust and confidence in policing among Black communities.
- Violence Against Women & Girls (VAWG) is a new framework, developed under the National Police Lead for VAWG, as a national focus on supporting forces to priorities VAWG-related crimes.

27. Home office departments

27.1 Border Force

27.2 Immigration Enforcement

27.3 Corporate and Delivery

27.4 Customer Services

27.5 Homeland Security Group

27.6 Migration and Borders Group

27.7 Public Safety Group

27.8 STAR and Home Office Chief Scientific Adviser

27.9 Strategy Directorate

28. Ministry of Justice departments

28.1 Ministry of Justice HQ

28.2 HM Prison & Probation Service (HMPPS)

28.3 HM Courts & Tribunal Service (HMCTS)

Appendix A: TERMS AND DEFINITIONS

Definition	Interpretation
AFA	Refers to the Armed Forces Act 2006 . The main law that governs the British military and its service justice system.
Anonymised Data	Means data in a form that cannot identify individuals and where any subsequent identification through its combination with other information is not likely to take place.
CCA	Refers to the Crime and Courts Act 2013 . The CCA sets out the functions and powers of the National Crime Agency.
Controller	Takes the definition within UK Data Protection Legislation: <i>“the natural or legal person, public authority, agency or other body which, along or jointly with others, determines the purposes and means of the processing of personal data”</i> .
Competent Authority	Takes the definition within UK Data Protection Legislation but can be summarised as meaning: • a person specified in Schedule 7 of the DPA; or • any other person if, and to the extent that, they have statutory functions to exercise public authority or public powers for the law enforcement purposes (Section 30(1) (b) of the DPA 2018).
Criminal Offence Data	Criminal offence data includes the type of data about criminal allegations, proceedings or convictions.
Consent	Freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data. Not to confused with “consent to participate”
Data	Means any data that includes personal data, special category data, criminal offence data as defined by the UK Data Protection Legislation and non-personal data (data that does not relate to and cannot identify an individual) that is collected for a legitimate business function by the Participants and when shared between the Participants can support the Participants to better deliver their respective business objectives and/or functions.
DPA	Data Protection Act 2018 .
DUAA	Data (Use and Access) Act 2025 .
UK Data Protection Legislation	In general, can be taken to mean the UK General Data Protection Regulation together with the Data Protection Act 2018 (DPA) and all secondary legislation made under it. These laws govern the way in which Controllers can process an individual's personal data and provide individuals' rights in relation to the processing of, and access to, their personal data.

	Specifically, “UK Data Protection Legislation” takes the meaning as at S3(9) Data Protection Act 2018 to include: a) the UK GDPR b) the Data Protection Act 2018 c) the DUAA 2025 d) regulations made under the DPA 2018 e) regulations made under section 2(2) of the European Communities Act 1972 which relate to the EU UK GDPR or the Law Enforcement Directive.
Data Protection Impact Assessment (DPIA)	A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection of any activity where personal data is processed (including Data Sharing).
Data Sharing Agreement (DSA)	A written document that sets out: the circumstances and purpose of a data sharing activity; a common set of standards to be adopted by the participants; and the roles and responsibilities of participants.
Data Subject	Means (as defined in the UK Data Protection Legislation) the identified or identifiable living person to whom personal data relates.
Data Subject Rights	Also known as ‘individuals’ rights. Under the UK Data Protection Legislation, Data Subjects have the following rights: • The right to be informed • The right of access • The right to rectification • The right to erasure • The right to restrict processing • The right to data portability • The right to object • Rights in relation to automated decision making and profiling Some rights are qualified, and some are absolute.
EIR / EIR(S)	Environmental Information Regulations 2004 and Environmental Information Regulation (Scotland) 2004
FOIA / FOI(S)	Freedom of Information Act 2000 and Freedom of Information (Scotland) Act 2002
General Purposes/Processing	Processing of personal data covered by the regime under the UK GDPR & Part 2 of the DPA (for General Processing).
UK General Data Protection Regulation (UK GDPR)	General Data Protection Regulation (European legislation) has been retained in UK law following the end of the transition period, this is now replaced by the UK GDPR. This legislation governs the processing of personal data. UK GDPR is defined as:

	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018
Human Rights Act 1998	Human Rights Act 1998 (legislation.gov.uk)
Information Commissioner	The regulator appointed by the Crown to promote public access to official information and protection of personal information. Compliance with the Data Protection Legislation is enforced by the Information Commissioner. They are supported by the Information Commissioner's Office .
Law Enforcement Purposes/Processing	Means (as defined in UK Data Protection Law) “... <i>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.</i> ”
Law	Means any applicable law, statute, byelaw, regulation, and order.
NCA Officer	For the purposes of this UDSA the meaning of NCA Officer deviates from the legal definition within the CCA. Within the UDSA NCA Officer is intended to refer to all those working for and on behalf of the NCA including contingent labour and specialist outsourced services NCA may use to fulfil its functions.
Non-Personal Information	Means information that does not relate to and does not identify a living individual.
Overarching ‘Umbrella Data Sharing Agreement’ (UDSA)	An umbrella document outlining high level arrangements with a data controller(s) where the intention/ expectation is that there will be a regular or significant amount of data sharing taking place involving personal data. The UDSA sets out the overarching principles of data sharing between the Participants and should be supported by Process-Specific Data Sharing Agreements where appropriate.
Participant(s)	The organisations and departments listed in Schedule 1 - Participants
Personal Data	Defined in the UK Data Protection Legislation as meaning: “any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or 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 Breach	A personal data breach is a “breach of security leading to the accidental or unlawful destruction, loss alteration, unauthorised disclosure of, or access to, personal data”

	transmitted stored or otherwise processed under this UDSA. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. Examples of serious personal data breaches may include: • accidental loss or damage to the personal data • damage or loss of personal data by means of malicious software/hacking • deliberate or knowing disclosure of personal data to a person not entitled to receive the data • emailing classified/sensitive information containing personal data to personal email accounts • leaving classified/sensitive papers containing personal data in an unsecure or publicly accessible area • using social networking sites to publish information containing personal data which may bring either Participant's organisations into disrepute • computing devices containing personal data being lost or stolen • alteration of personal data without permission and • loss of availability of personal data.
Privacy Information Notice (PIN)	A privacy notice is a public document from an organisation that explains how that organisation processes personal data and how it applies data protection principles.
Processor	Means (as defined in the UK Data Protection Legislation), any person who processes personal data on behalf of the Controller (other than an employee acting within the scope of their duties).
Process/Processed/Processing	Means (as defined in the UK Data Protection Legislation) the collecting, recording, storing, retrieving, amending altering, disclosing, deleting, archiving, destroying, or other operation performed on personal data.
Process-Specific Data Sharing Agreement (PDSA)	A purpose-specific information sharing document to manage specific process level information sharing activities. It sets out the circumstances and means by which information will be shared between Participants for specified purposes. Each PDSA will be arranged between the relevant Participants for each purpose-specific information sharing activity. A recommended template for PDSAs forms Annex A to this UDSA.
Pseudonymised Data	Means information where a unique identifier is used to replace/substitute any Personal Data, so as not to reveal an individual's 'real world' identity - and which can only be reversed by the Controller.

Sensitive Processing	For processing activities carried out for DPA Part 3 Law Enforcement Purposes, means (as defined in UK Data Protection Legislation): • The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; • The processing of genetic data for the purposes of uniquely identifying an individual • The processing of biometric data for the purposes of uniquely identifying an individual • The processing of data concerning health • The processing of data concerning an individual's sex life or sexual orientation.
Special Category Data	Means (as defined by UK Data Protection Legislation): • personal data revealing racial or ethnic origin; • personal data revealing political opinions; • personal data revealing religious or philosophical beliefs; • personal data revealing trade union membership; • genetic data; • biometric data (where used for identification purposes); • data concerning health; • data concerning a person's sex life; and • data concerning a person's sexual orientation.
Third Party	A person or group besides the Participants to this UDSA.