Ministry of Justice

Data sharing agreement (external)

THIS DATA SHARING AGREEMENT is made on the **16th day of May 2023**

BETWEEN

THE SECRETARY OF STATE FOR JUSTICE of 102 Petty France, London SW1H 9AJ ("MoJ" – The Receiving Party)

AND

GREATER MANCHESTER POLICE of Central Park, Manchester M40 5BP ("GMP" – The Disclosing Party)

AS WITNESS of which the parties have set their hands on the day and year first above written

SIGNED for and on behalf of THE SECRETARY OF STATE FOR JUSTICE By:

Name:[redacted]

Title: [redacted]

Signature: [redacted]

.....

SIGNED for and on behalf of GREATER MANCHESTER POLICE By:

Name:[redacted]

Title: [redacted]

Signature: [redacted]

.....

1 Definitions and interpretation

1.1 In this Agreement:

Communication	means a complaint, enquiry, notice, request or other communication (but excluding any Data Subject Request) relating to either party's obligations under any Data Protection Laws in connection with this Agreement and/or the Processing of any of the Shared Personal Data, including any compensation claim from a Data Subject or any notice, investigation or other action from a Data Protection Supervisory Authority relating to any of the foregoing;
Consent	means a freely given, specific, informed and unambiguous indication (by a statement or by a clear affirmative action) by which the relevant Data Subject has agreed to the relevant transfer(s) and/or Processing of the Shared Personal Data relating to them that has not been withdrawn. To the extent the relevant Shared Personal Data is Special Category Personal Data, this definition should be read as if the word 'unambiguous' above read 'unambiguous and explicit'. The terms "freely given", "specific", "informed", "unambiguous" and "explicit" in this definition shall be construed in accordance with Data Protection Laws;

Contact Point	means, in respect of each party, the person identified as such in accordance with paragraph 1 of Appendix 5 of this Agreement;
Controller	has the meaning given in Data Protection Laws;
Data Protection Laws	means, as applicable to either party: (a) the UK GDPR; (b) the Data Protection Act 2018; (c) the Privacy and Electronic Communications (EC Directive) Regulations 2003; (d) any other applicable law relating to the Processing, privacy and/or use of Personal Data; (e) any laws which implement or supplement any such laws; and (f) any laws that replace, extend, re-enact, consolidate or amend any of the foregoing;
Data Protection Supervisory Authority	means any regulator, authority or body responsible for administering Data Protection Laws;
Data Subject	has the meaning given in Data Protection Laws;
Data Subject Request	means a request made by a Data Subject to exercise any right(s) of Data Subjects under Chapter III of the GDPR in relation to any of the Shared Personal Data or concerning the Processing of such data;
Disclosing Party	means each party to the extent it discloses or otherwise makes accessible any Shared Personal Data to the Receiving party;
GDPR	means the General Data Protection Regulation, Regulation (EU) 2016/679, as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time);
Permitted Lawful Basis	means: (a) the agreed lawful basis under Article 6(1) of the GDPR under which the Shared Personal Data is shared by the Disclosing Party with the Receiving Party and Processed by the Receiving Party. For this project, the legal basis is "In the Public Interest"; and (b) the additional condition under Article 9(2) of the GDPR under which the Shared Personal Data that is Special Category Personal Data is shared by the Disclosing Party with the Receiving Party and Processed by the Receiving Party. For this project, the additional condition is "Of substantial Public Interest", and in particular "Preventing or detecting unlawful acts" and "Protecting the public";
Permitted Purpose	means the Receiving Party's intended and authorised use of the relevant Received Personal Data. For this project the purpose is to use the data to: (a) To identify those who demonstrate behaviours or tendencies which tend to be in line with committing homicide, and (b) To identify those who have a previous history of committing violent offences and offences linked to going onto commit homicide;
Permitted Recipients	means the relevant Receiving Party's employees who need access to the Received Personal Data for the Permitted Purpose;
Personal Data	has the meaning given in Data Protection Laws;
Personal Data Breach	has the meaning given in Data Protection Laws;
Processing	has the meaning given in Data Protection Laws;
Processor	has the meaning given in Data Protection Laws;
Received Personal Data	means Shared Personal Data in respect of which the relevant party is the Receiving Party;
Receiving Party	means each party to the extent it receives or accesses any Shared Personal Data

disclosed or made available by the Disclosing Party;

Shared Personal Data	means Personal Data made available by the Disclosing party to the Receiving Party for the Permitted Purpose;
Special Category Personal Data	means special categories of Personal Data as referred to in Data Protection Laws; and
UK Law	means applicable law of the United Kingdom or of a part of the United Kingdom.

2 Status of this Agreement and the parties

Each party shall be an Independent Controller of the Shared Personal Data. If the parties share the Shared Personal Data, it shall be shared and managed in accordance with the terms of this Agreement.

3 Compliance with Data Protection Laws

3.1 Subject to compliance by the other party with its express obligations in other provisions of this Agreement, each party shall at all times comply with all Data Protection Laws in connection with the exercise and performance of its respective rights and obligations under this Agreement.

3.2 This Agreement allocates certain rights and responsibilities among the parties as enforceable contractual obligations between themselves, however nothing in this Agreement is intended to limit or exclude either party's responsibilities or liabilities under Data Protection Laws.

4 Agreed basis for sharing

4.1 The parties have determined that it is necessary to share the Shared Personal Data in order to achieve the Permitted Purpose.

4.2 The parties agree that this Agreement relates to:

(a) A one-off data sharing of the Receiving Party's cohort data, which will be used to perform a project feasibility study. This data will be linked with data, which is internal to the Receiving Party, to determine the cohort size for the project. If at this point the Receiving Party finds that the cohort size is too small, they will not continue to the second part in this Agreement

(b) A one-off data sharing of the Receiving Party's criminal history data for the much-smaller cohort for the project. Once this dataset is linked to four datasets, which are internal to the Receiving Party, the entire data will be anonymised. The data will be used as possible predictive variables in the data science project. If at this point any data fields are shown to have no or little predictive power, they will be removed from the model.

4.3 The parties have documented additional details relating to the sharing of the Shared Personal Data in Appendix 2 of this Agreement, which includes:

4.3.1 the aims of each party in sharing the Shared Personal Data;

4.3.2 why sharing the Shared Personal Data on the terms of this Agreement is necessary to achieve those aims;

4.3.3 the benefits to society of the parties sharing the Shared Personal Data; and

4.3.4 A Data Protection Impact Assessment undertaken by the Receiving Party, a Data Protection Impact Assessment undertaken by the Disclosing Party, and a Movement Form for the Analytical Platform that will host the data within the Receiving Party's systems.

5 General obligations

5.1 The Receiving Party shall undertake all Processing of Received Personal Data only:

5.1.1 for the Permitted Purpose in accordance with this Agreement and in all respects in accordance with Data Protection Laws; and

5.1.2 to the extent consistent with the Permitted Lawful Basis,

except to the extent otherwise required by UK Law.

5.2 The parties agree that in respect of Shared Personal Data, the relevant Disclosing Party:

5.2.1 is, as between the parties and subject to paragraphs 5.3 and 9.1, the primary point of contact for Data Subjects;

5.2.2 subject to paragraphs 5.3 and 9.1, shall direct Data Subjects and queries about the Shared Personal Data to its Information Compliance and Records Management Unit;

5.2.3 shall ensure that the Shared Personal Data has been collected, Processed and transferred in accordance with the Data Protection Laws as applicable to that data at all times prior to the receipt of that data by the Receiving Party;

5.2.4 shall ensure the Shared Personal Data is accurate and up-to-date when disclosed or made accessible to the relevant Receiving Party and shall promptly notify the Receiving Party if such Shared Personal Data becomes inaccurate or out of date during the term of this Agreement;

5.2.5 is solely responsible for both parties' compliance with all duties to provide information to Data Subjects under Articles 5(1)(a), 13 and 14 of the GDPR or any similar Data Protection Laws, including as required for all Processing of Shared Personal Data by the Receiving Party for the Permitted Purpose on the Permitted Lawful Basis in accordance with this Agreement and shall comply with its respective obligations in Appendix 4. Given the project's legal basis is "In the Public Interest", there is no obligation to pre-emptively inform all Data Subjects of the project;

5.2.6 shall ensure that the Shared Personal Data when transferred to the Receiving Party in connection with this Agreement:

(a) is not subject (or potentially subject) to any laws giving effect to Article 71 (Protection of personal data) of the agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community; and

(b) is not subject to the laws of any jurisdiction outside of the United Kingdom;

5.2.7 without prejudice to its other obligations, shall ensure that it is entitled to transfer the Shared Personal Data to the Receiving Party and that the Receiving Party is entitled under all applicable laws and legal theories to Process the Shared Personal Data for the Permitted Purpose in accordance with the terms of this Agreement;

5.2.8 shall promptly notify the Receiving Party if a relevant Data Subject has requested that their Shared Personal Data is no longer Processed by either party for the Permitted Purpose;

5.2.9 is solely responsible for ensuring that where the Shared Personal Data was received by the Disclosing Party from a third party, or has been Processed by a third party on behalf of the Disclosing Party, it has in place arrangements with those third parties:

(a) as required by all Data Protection Laws (including, where applicable, Articles 26, 28 and 32 of the GDPR);

(b) which are adequate to permit the Disclosing Party to share the Shared Personal Data with the Receiving Party (and its Permitted Recipients) under all Data Protection Laws; and

(c) as required for the Receiving Party (and its Permitted Recipients) to Process such data in accordance with this Agreement; and

5.2.10 where appropriate, can make available to Data Subjects the essence of this Agreement (and notify them of any changes to it) as required by Article 26 of the GDPR. Confidential Information shall be redacted if the legal basis for including is no longer true.

5.3 Notwithstanding the terms of this Agreement, the parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Laws against any relevant party as Controller.

5.4 Each party shall use its reasonable endeavours to assist the other to comply with any obligations under all Data Protection Laws in connection with this Agreement and shall not perform its obligations under this Agreement in such a way as to cause the other party to breach any of the other party's obligations under applicable Data Protection Laws to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

5.5 Without prejudice to any other obligation, if either party becomes aware any of the Shared Personal Data is inaccurate or out of date, it shall promptly notify the other.

6 Technical and organisational measures

6.1 The Receiving Party shall at all times:

6.1.1 put in place and maintain appropriate technical and organisational measures as required by Data Protection Laws;

6.1.2 implement and maintain appropriate technical and organisational measures to protect the Received Personal Data in its possession or control against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access, taking into account:

(a) the nature of the data to be protected;

(b) the harm that might result from any failure to so protect the Received Personal Data;

(c) the state of technological development; and

(d) the cost of implementing any measures;

6.1.3 ensure that it has the capability (technological and otherwise), to the extent required by Data Protection Laws, to:

(a) provide, correct or delete at the request of a Data Subject all the Received Personal Data relating to that Data Subject; and

(b) comply with any Data Subject Requests; and

6.1.4 without prejudice to any other obligation in this paragraph 6, implement and comply with the technical and organisational measures specified in Appendix 3 of this Agreement.

6.2 Each party shall comply with its respective obligations, and may exercise its respective rights and remedies, under Appendix 3 of this Agreement.

7 Third party Processing

7.1 The Receiving Party agrees not to disclose or transfer Received Personal Data to any third party.

7.2 The Receiving Party will perform all Processing relating to the Received Data and agrees to not engage any third party in the Processing stage.

8 International transfers

The Receiving Party shall not transfer Received Personal Data to any country or territory outside the United Kingdom or to any international organisation (as defined in the GDPR), except to the extent required by UK Law or with the Disclosing Party's express prior written consent. For the purposes of this paragraph 8 '**transfer**' bears the same meaning as the word 'transfer' in Article 44 of the GDPR.

9 Dealing with Data Subject Requests and Communications

9.1 Responsibility for complying with any Data Subject Request or Communication falls on the party which first received such Data Subject Request or Communication. In complying with any Data Subject Request or addressing any Communication each party shall comply with its obligations as outlined in *the section on 'Detailed procedures for addressing Data Subject Requests and Communications' in* Appendix 7.

9.2 If either party receives a Communication relating to the Shared Personal Data Processed by (or on behalf of) the other party it shall to the extent lawful under UK Law:

9.2.1 promptly notify the Information Compliance and Records Management Unit or the Data Protection Team at the other party; and

9.2.2 consult with the other party in advance of giving any response, to the extent reasonably practicable.

9.3 Each party shall use all reasonable endeavours to provide the other party with full and prompt co-operation and assistance in relation to any Data Subject Request or Communication made to enable the other party to comply with the relevant timescales set out in Data Protection Laws and to find an efficient, timely and amicable solution to any issues arising out of any Data Subject Request or Communication. Without prejudice to the generality of the foregoing, the other party shall respond to any request for co-operation or assistance under this paragraph 9.3 within three business days.

10 Personal Data Breaches

10.1 Each party shall promptly (and in any event within 24 hours) notify the Disclosing Party if it suspects or becomes aware of any actual or threatened occurrence of any Personal Data Breach in respect of any Received Personal Data which it processes as Receiving Party. In such circumstances, the relevant Receiving Party shall promptly provide (to the extent permitted by UK Law):

10.1.1 sufficient information as the Disclosing Party reasonably requires to meet any obligations to report a Personal Data Breach under Data Protection Laws (in a timescale which facilitates such compliance);

10.1.2 the Data Protection Supervisory Authorities investigating the Personal Data Breach with complete information as requested by those Data Protection Supervisory Authorities from time to time;

10.1.3 all reasonable assistance the Disclosing Party (or its advisors) requires, including:

(a) co-operation with Data Protection Supervisory Authorities (including with investigations or actions to mitigate or remediate the Personal Data Breach);

(b) making available all relevant data and records required for either party to comply with Data Protection Laws or as otherwise reasonably required by the Disclosing Party;

(c) taking such reasonable steps as are directed by the Disclosing Party to assist in the investigation, mitigation and remediation of a Personal Data Breach (which may include providing the Disclosing Party with physical access to any facilities affected and facilitating the interview of staff and others involved in the matter); and

(d) co-ordination with the Disclosing Party regarding the management of public relations and public statements relating to the Personal Data Breach.

10.2 The Receiving Party's obligations under this paragraph 10 shall be performed at the Receiving Party's cost and expense.

11 Data protection impact assessments

11.1 The Parties have completed a Data Protection Impact Assessment in respect of the planned sharing of the Shared Personal Data under this Agreement and have agreed that this Agreement will assist with mitigating certain risks that have been identified.

11.2 Where a party considers that a new Data Protection Impact Assessment or changes to the current one are necessary for compliance with Data Protection Law, the other Party shall provide such reasonable assistance as that Party may reasonably require.

11.3 The assistance referred to in paragraph 11.2 may include:

11.3.1 a systematic description of the envisaged Processing operations and Permitted Purpose of the Processing of the Shared Personal Data;

11.3.2 an assessment of the necessity and proportionality of the Processing operations;

11.3.3 an assessment of the risks to the rights and freedoms of Data Subjects;

11.3.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of the Shared Personal Data; and

11.3.5 any prior consultation with the relevant Data Protection Supervisory Authority which may be necessary.

12 Records

Each party shall maintain complete, accurate and up to date written records of all its Processing of the Shared Personal Data and as necessary to demonstrate its compliance with this Agreement and all Data Protection Laws.

13 Governance and review

Prior to sharing the Shared Personal Data, the parties shall establish, and then comply with and maintain, the arrangements set out in Appendix 5 of this Agreement until[*the earlier of the termination or expiry of this Agreement*].

14 Additional arrangements

Each party shall comply with its respective obligations, and may exercise its respective rights and remedies, under Appendix 7 of this Agreement.

15 Audit

15.1 Each party shall:

15.1.1 make available to the other party such information as is reasonably required to demonstrate that party's compliance with its obligations under this Agreement;

15.1.2 upon prior notice allow for, permit and contribute to audits, including inspections, by the other party (or another auditor mandated by the other party) during normal business hours to the extent necessary to verify the audited party's compliance with its obligations under this Agreement; and

15.1.3 provide (or procure) access to all relevant systems, personnel, business premises and records for the purposes of each such audit or inspection referred to in paragraph 15.1.2 and provide (and procure) all further reasonable co-operation, access and assistance in relation to any such audit or inspection.

15.2 Each party shall allow the other to exercise its rights at paragraph 15.1 in the period up to one year after the termination or expiry of this Agreement.

15.3 When conducting audits and inspections, the relevant party conducting the audit or inspection shall comply with the other party's reasonable directions in order to minimise disruption to the other party's business and to safeguard the confidentiality of the other party's Confidential Information. The party subject to the audit or inspection may require any third parties conducting such audit or inspection to enter into direct confidentiality undertakings with it on terms that are substantially the same as the confidentiality obligations in this Agreement.

16 Retention

16.1 Subject to paragraph 16.2 and except as required by UK Law, each party shall retain the Received Personal Data in accordance with the retention periods identified for the specific element of the Shared Personal Data in accordance with Appendix 1 of this Agreement.

16.2 Except as required by UK Law, the parties shall, to the extent they are Receiving Party:

16.2.1 subject to paragraphs 16.2.2 to 16.2.3 (inclusive), Process all Received Personal Data for no longer than such Processing is necessary for the Permitted Purpose and compliant with this Agreement and all Data Protection Laws;

16.2.2 cease to Process all Received Personal Data on the earlier of termination or expiry of this Agreement; and

16.2.3 immediately, confidentially and securely destroy or dispose of all Received Personal Data (and all copies) in its possession or control that can no longer be Processed in accordance with this Agreement.

17 Costs

Except as expressly stated in this Agreement, each party shall pay its own costs and expenses incurred in connection with the negotiation, preparation, signature and performance of this Agreement.

APPENDIX 1
THE SHARED PERSONAL DATA

1 Shared Personal Data to be shared by the Disclosing Party, GMP, with the Receiving Part, MOJ.

Reference:	Person-level data to check cohort size
Subject matter of Personal Data to be shared	Structured tabular data containing personal data from local police data, which will be used to link record between GMP's and MOJ's systems. The data contains information for persons who have had contact with Greater Manchester Police before 01/01/2015 and are still on record within the legacy system. If the data was perfect quality, each row would represent a different person, but we are aware of duplication errors and have incorporated this limitation within the Processing of the data.
Type of Personal Data to be shared	The data fields within the Shared Personal Data are: * **First Name** * **Last Name** * **Date of Birth** * **Gender** - Female/Male/Other categories * **Ethnicity** - White/Black/Mixed/Asian/Other categories * **Person Citizen ID** (the Police identifier that will be used to link the two datasets the Disclosing Party provides) * **PNC ID** (only if the Disclosing Party judge the quality of this field is sufficient to use as a linking tool)
Special categories of Personal Data in this data	The only special category within the Shared Personal Data is: * Ethnicity (this variable has been shown to have high linking power when using an internal MOJ algorithm for probabilistic linking between other datasets) * Criminal Offence Data (in relation to warning markers/flags)
Categories of Data Subject	People who have had contact with Greater Manchester Police before 01/01/2015 in the role of either suspect, victim, witness, missing person or of safeguarding concern.
Lawful basis for sharing data (GMP)	**DPA Part 3 law enforcement processing:** It is understood that the vast majority of personal data processing undertaken within the Homicide predictor modelling project will fall under Part 3, law enforcement processing, as below: **Section 31** – Law Enforcement purposes - namely the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, includes the safeguarding against and the prevention of threats to public security. **Section 35** - The processing of personal data for a law enforcement purpose is lawful only if and to the extent that it is based on law and either: (a) the data subject has given consent to the processing for that purpose, or (b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority. Sensitive data for law enforcement purposes may only be carried out, the controller has an appropriate policy document in place and either: (a) the data subject has given consent to the processing, or (b) the processing is strictly necessary for the law enforcement purpose and the processing meets at least one of the conditions from Schedule 8 of the DPA. Full details of Schedule 8 can be found at: *https://ico.org.uk/for-*

Reference:	Person-level data to check cohort size
	organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing/' The lawful conditions from Schedule 8 for this provision are:- *Statutory etc. purposes* - Processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest. The processing is plainly carried out for reasons of substantial public interest, these being to protect the public, prevent and detect crime. **GDPR/DPA Part 2 general processing:** Where personal data processing in the Homicide predictor modelling project falls outside of the law enforcement purposes, processing must still be necessary for a wider policing purpose, as defined by MoPI, and as per the below conditions. **Article 6(1)(e)** GDPR – performance of a task carried out in the public interest. In some circumstances personal data may be processed that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or health data, which is defined as 'Special Category Personal Data'. Additional legitimising conditions apply for the processing of that data, which are clarified below: **Article 9(2)(g)** GDPR – processing is necessary for reasons of substantial public interest. As Art 9(2)(g) applies, we must meet a schedule 1 Part 2 Condition(s). Please see below: Schedule 1, Part 2(6) DPA – statutory/government purposes (policing task in the substantial public interest) Schedule 1, Part 2(10) DPA – preventing or detecting unlawful acts Schedule 1, Part 2(18) DPA – safeguarding of children and individuals at risk **Article10 GDPR** – processing of criminal convictions and offences must only be processed under the control of official authority or authorised by law. s10(5) DPA – processing is authorised by law only if it meets a condition in Part 1, 2 or 3 of Schedule 1. Schedule 1, Part 2(6) – statutory/government purposes (policing task in the substantial public interest) Schedule 1, Part 2(10) – preventing or detecting unlawful acts Schedule 1, Part 2(18) – safeguarding of children and individuals at risk

Reference:	Person-level data to check cohort size
	Applicable acts/legislation: • **Crime and Disorder Act 1998** – Section 17 (duty to consider crime and disorder implications) and Section 115 (disclosure of information) for the purpose of prevention and reduction of crime, disorder and antisocial behaviour. • **Common law duty** of disclosure in the interests of policing purposes, following a data protection and human rights assessment **Human Rights Act 1998** (The data will be anonymised before any modelling begins. No individual or group will be identifiable in the final outputs)
Lawful basis for processing data (MoJ)	Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller The MoJ is permitted to process data supplied by the police, the Crown Prosecution Service (CPS), courts and prisons by virtue of its common law powers for the administration of justice. These general powers are supported by various legislative provisions which allow the collection and sharing of information for offender management as well as the establishment and execution of services relevant to the MoJ's Executive Agencies and ALBs. Research and analysis are carried out under Article 9(2)(j): "Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject." This provision is supported by section 4, Part 1 of Schedule 1 of the DPA 2018. The MoJ processes criminal offence data under the control of official authority in accordance with Article 10 of the UK GDPR.
Who in Disclosing Party shares the data?	[redacted]
Date planned for sharing	w/c 03/04/2023
How will it be shared?	The data will be transferred using an MOJ tool, the data uploader. It enables secure transfer of csv data chunked into 5GB segments. Data will be stored in an S3 bucket in an SQL like structure with one database at the top level, which contains one or more data tables. Data is encrypted at Transit and the Data stored will be encrypted within the bucket. There is a web access firewall (WIP). There are cloud trails and lambda upload cloudwatch logs, which are available. Access to both the data uploader and then the data folder is managed via a project access file. Nobody who is not listed in this Agreement will have access to the data.
Who in the Receiving Party receives the data?	The lead analyst at MOJ is [redacted] team will be the only people listed within the access file to the S3 buckets. The only team members with permissions will be: * [redacted]
What happens with the data when it is received?	The data will be uploaded by the Disclosing Party to the MOJ secure network using the data uploader. The data will be encrypted within an S3 bucket. The data will then be linked to internal data on the Analytical Platform to check the cohort size of people in both the local police's data and on the Probation caseload of interest. At this point a decision will be made whether the cohort size is large enough to process with the project. If it is, then a derivative

Reference:	Person-level data to check cohort size
	dataset will be created with the Person Citizen identifiers for all people that become the cohort for the project. This dataset will be saved into the same encrypted S3 bucket and shared back with [redacted] to add the police contact history for this cohort.
What retention period shall be applied to that data?	The Receiving Party plans to retain the data until December 2024, 6 months after the end of the project. This will ensure we have the capability to answer any follow-up questions or follow new leads after presenting our research and findings. The Receiving Party plans to have reviews within this 6 month period in case the full retention period is not needed.

Shared Personal Data to be shared by [*Party 2*] with [*Party 1*]

Reference:	Police Contact History for the agreed cohort
Subject matter of Personal Data to be shared	Structured tabular data containing police contact history from local police data, which will be used to create possible predictive variables for a data science project. The data contains information for persons who have had contact with Greater Manchester Police before 01/01/2015. If the data was perfect quality, each row would represent a different person, but we are aware of duplication errors and have incorporated this limitation within the Processing of the data. We are also aware of many data quality issues with this legacy data source due to many system restructurings since then. We plan to work in an agile and flexible way to allow for changes in data variables selection, and we plan to work closely with and be guided by GMP's analysts and Information Compliance Records Management Unit.
Type of Personal Data to be shared	The data fields required will be agreed after the cohort size discovery is completed. This is because there is a lot of uncertainty around the data quality in the legacy dataset at GMP and there is also a restriction on the amount of time that GMP colleagues can allocate to this project. We have undergone a prioritisation exercise and will aim to obtain as many of the "Must have" and "Should have" fields in the following list. <u>Must have</u>: Person Citizen ID (for matching to the internal MOJ dataset) Number of previous homicide classification before 01/01/2015 Number of previous Violence with injury classification before 01/01/2015 Number of previous Possession of weapon offences classification before 01/01/2015 Number of all classifications before 01/01/2015 Number of Cautions before 01/01/2015 Number of Convictions before 01/01/2015 Number of Final Warnings before 01/01/2015 Number of Reprimands before 01/01/2015 Number of Penalties before 01/01/2015 Number of Penalty Notices before 01/01/2015 Number of Fines before 01/01/2015 Number of Charges before 01/01/2015 Number of Arrests before 01/01/2015 Suspect of Homicide Flag before 01/01/2015 Suspect of Criminal damage and arson offences Flag before 01/01/2015 Suspect of Possession of weapon offences Flag before 01/01/2015 Suspect of Stalking and harassment Flag before 01/01/2015 Suspect of Violence with injury Flag before 01/01/2015 Suspect of Violent Offence Flag before 01/01/2015 Age first appearing as Witness in System before 01/01/2015 Age first appearing as Victim in System before 01/01/2015 Age first appearing as Offender in System before 01/01/2015 Age first appearing as Missing in System before 01/01/2015 Age first appearing as Suspect in System before 01/01/2015 Age of first contact with Police before 01/01/2015

Reference:	Police Contact History for the agreed cohort
	Number of Crimed domestic abuse incidents before 01/01/2015 Domestic abuse association as victim flag before 01/01/2015 Domestic abuse association as perpetrator flag before 01/01/2015 Alleged Perpetrator Flag before 01/01/2015 Domestic_Abuse_Flag before 01/01/2015 Repeat_Domestic_Abuse_Flag before 01/01/2015 Repeat Victim Flag before 01/01/2015 Victim of 10+ Harm Flag before 01/01/2015 Victim of 730+ Harm Flag before 01/01/2015 Victim of Homicide Flag before 01/01/2015 Violent flag before 01/01/2015 Weapons flag before 01/01/2015 Use Knife Or Sharp Instruments Qualifier Flag before 01/01/2015 Firearms flag before 01/01/2015 Seriously Dangerous Offender Status before 01/01/2015 Hate_Crime_Flag before 01/01/2015 ViSOR Subject Marker Flag before 01/01/2015 Mental health warning flag before 01/01/2015 Alcohol_Influence_Flag before 01/01/2015 Drugs_Influence_Flag before 01/01/2015 Safeguarding flag before 01/01/2015 <u>Should have</u>: Prolific Offender Marker Flag before 01/01/2015 Repeat suspect Flag before 01/01/2015 Sex Offender Marker Flag before 01/01/2015 Conceals warning flag before 01/01/2015 Explosives flag before 01/01/2015 GMP Latest Outcome before 01/01/2015 Number of previous Violence without injury classification before 01/01/2015 Number of previous Trafficking of drugs classification before 01/01/2015 Breaches Bail Conditions Marker Flag before 01/01/2015 Self harm flag before 01/01/2015 Suicidal flag before 01/01/2015 Vulnerable flag before 01/01/2015 Disability Qualifier Flag before 01/01/2015 Racial Qualifier Flag before 01/01/2015 Religion Or Belief Qualifier Flag before 01/01/2015 Perceived Religion Targeted Qualifier before 01/01/2015 Honour Incident Qualifier Flag before 01/01/2015 Suspect of 10+ Harm Flag before 01/01/2015 Suspect of 730+ Harm Flag before 01/01/2015 Victim of Criminal damage and arson offences Flag before 01/01/2015 Victim of Death or serious injury caused by unlawful driving Flag before 01/01/2015 Victim of Possession of drugs Flag before 01/01/2015 Victim of Possession of weapon offences Flag before 01/01/2015 Victim of Stalking and harassment Flag before 01/01/2015 Victim of Trafficking of drugs Flag before 01/01/2015 Victim of Violence with injury Flag before 01/01/2015 Victim of Violence without injury Flag before 01/01/2015 Victim of Violent Offence Flag before 01/01/2015 Suspect of Possession of drugs Flag before 01/01/2015

Reference:	Police Contact History for the agreed cohort
	Suspect of Trafficking of drugs Flag before 01/01/2015 Suspect of Violence without injury Flag before 01/01/2015 Suspect of Death or serious injury caused by unlawful driving Flag before 01/01/2015 Crime as Victim whilst Age under 18 Flag before 01/01/2015 Crime as Offender whilst Age under 18 Flag before 01/01/2015 PPI Flag before 01/01/2015
Special categories of Personal Data in this data	The special categories within the Shared Personal Data are: (a) Health markers (which are expected to have significant predictive power) such as: * Mental Health flag * Addiction flags * Self harm/Suicide/Vulnerable flags * Disability flag (b) Beliefs and ideology markers (which are also expected to have significant predictive power) such as: * Hate crime flag * Racial Qualifier flag * Religion or Belief Qualifier flag * Honour Incident Qualifier flag
Categories of Data Subject	People who have (a) had contact with Greater Manchester Police before 01/01/2015 in the role of either suspect, victim, witness, missing person or of safeguarding concern, and (b) are within the cohort for the project, which is defined as people who had a record on the Probation caseload before 01/01/2015 and had a completed Layer 3 Oasys assessment before 01/01/2015. We estimate that the cohort size will be between 5,000 and 15,000 depending on the data quality of the identifiers and personal characteristics that are used to link in the first phase of the project.
Lawful basis for sharing data (GMP)	**DPA Part 3 law enforcement processing:** It is understood that the vast majority of personal data processing undertaken within the Homicide predictor modelling project will fall under Part 3, law enforcement processing, as below: **Section 31** – Law Enforcement purposes - namely the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, includes the safeguarding against and the prevention of threats to public security. **Section 35** - The processing of personal data for a law enforcement purpose is lawful only if and to the extent that it is based on law and either: (a) the data subject has given consent to the processing for that purpose, or (b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority. Sensitive data for law enforcement purposes may only be carried out, the controller has an appropriate policy document in place and either: (a) the data subject has given consent to the processing, or (b) the processing is strictly necessary for the law enforcement purpose and the processing meets at least one of the conditions from Schedule 8 of the DPA. Full details of Schedule 8 can be found at: *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing/* The lawful conditions from Schedule 8 for this provision are:-

Reference:	Police Contact History for the agreed cohort
	Statutory etc. purposes - Processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest. The processing is plainly carried out for reasons of substantial public interest, these being to protect the public, prevent and detect crime. **GDPR/DPA Part 2 general processing**: Where personal data processing in the Homicide predictor modelling project falls outside of the law enforcement purposes, processing must still be necessary for a wider policing purpose, as defined by MoPI, and as per the below conditions. **Article 6(1)(e)** GDPR – performance of a task carried out in the public interest. In some circumstances personal data may be processed that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or health data, which is defined as 'Special Category Personal Data'. Additional legitimising conditions apply for the processing of that data, which are clarified below: **Article 9(2)(g)** GDPR – processing is necessary for reasons of substantial public interest. As Art 9(2)(g) applies, we must meet a schedule 1 Part 2 Condition(s). Please see below: Schedule 1, Part 2(6) DPA – statutory/government purposes (policing task in the substantial public interest) Schedule 1, Part 2(10) DPA – preventing or detecting unlawful acts Schedule 1, Part 2(18) DPA – safeguarding of children and individuals at risk **Article10 GDPR** – processing of criminal convictions and offences must only be processed under the control of official authority or authorised by law. s10(5) DPA – processing is authorised by law only if it meets a condition in Part 1, 2 or 3 of Schedule 1. Schedule 1, Part 2(6) – statutory/government purposes (policing task in the substantial public interest) Schedule 1, Part 2(10) – preventing or detecting unlawful acts Schedule 1, Part 2(18) – safeguarding of children and individuals at risk Applicable acts/legislation: • **Crime and Disorder Act 1998** - Section 17 (duty to consider crime and disorder implications) and Section 115 (disclosure of information) for the purpose of prevention and reduction of crime, disorder and antisocial behaviour. • **Common law duty** of disclosure in the interests of policing purposes, following a

Reference:	Police Contact History for the agreed cohort
	data protection and human rights assessment **Human Rights Act 1998** (The data will be anonymised before any modelling begins. No individual or group will be identifiable in the final outputs)
Lawful basis for processing data (MoJ)	Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller The MoJ is permitted to process data supplied by the police, the Crown Prosecution Service (CPS), courts and prisons by virtue of its common law powers for the administration of justice. These general powers are supported by various legislative provisions which allow the collection and sharing of information for offender management as well as the establishment and execution of services relevant to the MoJ's Executive Agencies and ALBs. Research and analysis are carried out under Article 9(2)(j): "processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject." This provision is supported by section 4, Part 1 of Schedule 1 of the DPA 2018. The MoJ processes criminal offence data under the control of official authority in accordance with Article 10 of the UK GDPR.
Who in Disclosing Party shares the data?	[redacted] Greater Manchester Police
Date planned for sharing	w/c 05/06/2023
How will it be shared?	The data will be transferred using an MOJ tool, the data uploader. It enables secure transfer of csv data chunked into 5GB segments. Data will be stored in an S3 bucket in an SQL like structure with one database at the top level, which contains one or more data tables. Data is encrypted at Transit and the Data stored will be encrypted within the bucket. There is a web access firewall (WIP). There are cloud trails and lambda upload cloudwatch logs, which are available. Access to both the data uploader and then the data folder is managed via a project access file. Nobody who is not listed in this Agreement will have access to the data.
Who in the Receiving Party receives the data?	[redacted] be the only people listed within the access file to the S3 buckets. The only team members with permissions will be: [redacted]
What happens with the data when it is received?	The data will be uploaded by the Disclosing Party to the MOJ secure network using the data uploader. The data will be encrypted within an S3 bucket. The data will then be linked to internal data on the Analytical Platform and any derivative data or linked data will be saved back into the encrypted S3 bucket. Once all internal data is joined, the master dataset will be anonymised and saved in a different S3 bucket. From there the team will develop several data science models to test different hypotheses.
What retention period shall be applied to that data?	The Receiving Party plans to retain the data until December 2024, 6 months after the end of the project. This will ensure we have the capability to answer any follow-up questions or follow new leads after presenting our research and findings. The Receiving Party plans to have reviews within this 6 month period in case the full retention period is not needed.

APPENDIX 2
FURTHER DETAILS OF THE PERSONAL DATA SHARING

1 Data sharing objectives

The parties have determined the following aims and objectives of sharing the Shared Personal Data for the Permitted Purpose: to develop better tools for predicting the risk of homicide by including local police data, to evidence the need for more cross-unit collaboration and to enable further future research like this project.

2 Necessity

The parties have determined that sharing the Shared Personal Data on the terms of this Agreement is necessary to achieve those aims because: (a) MOJ data is not as rich as local police data when it comes to non-convictions and local police interactions, which are expected to provide predictive power when developing a risk predictor for homicide, and (b) the personal characteristics and identifiers enable linking between GMP and MOJ data. The Shared Personal Data will ensure that the predictive variables cover a fuller picture of offender's criminal journeys and we expect that it will lead to significant impact within the project.

3 Benefits of data sharing

The parties have determined the following benefits will be derived from sharing the Shared Personal Data: (a) a benefit to the public in identification and targeting those at risk of committing homicide, a priority offence group for the Crime and Justice Taskforce. In particular, the project aims to contribute towards "Preventing or detecting unlawful acts" and "Protecting the public".

4 Risks of data sharing and mitigation measures

4.1 The Disclosing and Receiving Parties will act as Independent Controllers. They are both conducting their own Data Protection Impact Assessments in respect of the sharing arrangements set out in this Agreement.

MOJ's DPIA completion date: expected to be 01/04/2023

GMP's DPIA completion date: TBC

4.2 The parties have determined the following risks may arise from sharing the Shared Personal Data, and have agreed measures to remove or mitigate such risks, including those measures set out in this Agreement:

Organisational risk: results from the analysis being misinterpreted or misused when setting new policy or new strategies	**Likelihood:** (Remote, possible or probable) **Severity:** (Minimal, significant or severe) **Overall Risk:** (Low, medium or high)	We will ensure that the work's results are quality assured and peer reviewed. Any significant outputs will be documented in a single source of the truth, which will also include any assumptions, caveats and limitations in relation to the outputs. We will set a high expectation for transparency with the steering board. We will save all code in Github to enable reproducibility and audit.
Compliance risk: pressure to widen the scope of the project and use the data for additional modelling	**Likelihood:** (Remote, possible or probable) **Severity:** (Minimal, significant or severe) **Overall Risk:** (Low, medium or high)	The project has very specific aims and its funding is signed off for limited time only. We plan to delete all GMP data once the project is finished. Any further analysis using this data will go through another DPIA process.

APPENDIX 3
TECHNICAL AND ORGANISATIONAL MEASURES

1 Security management

Without prejudice to its other obligations, the parties shall implement and maintain at least the following technical and organisational security measures, actively to ensure the safety and security of the Protected Data:

1.1 Technical and organisational measures to ensure a level of security appropriate to the risk, normally including:

1.1.1 the pseudonymisation and encryption of personal data;

1.1.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

1.1.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

1.1.4 process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

1.1.5 prompt and comprehensive maintenance of the measure to ensure currency and validity against risks.

1.2 The measures shall demonstrably take into account the state of the art, the costs of implementation, the consequences of impact, and the nature, scope, context and purposes of processing of Protected Data to be carried out under or in connection with this agreement, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

1.3 In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, storage or transmission of personal data arising from unplanned or unmanaged activities such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

1.4 Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 of the UK GDPR may be used as an element by which to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

1.5 Without prejudice to its other obligations, the Supplier shall normally implement National Cyber Security Centre SaaS security principles outlined here: SaaS security principles - NCSC.GOV.UK

2 Personnel

2.1 The Receiving Party will ensure the Processing of the Received Personal Data by natural persons shall be limited to its employees and the employees of its Permitted Recipients (collectively, **personnel**) that need to Process it for the relevant Permitted Purpose in accordance with this Agreement and that all such personnel:

2.1.1 are reliable and have undergone adequate training in the use, care, protection and handling of Received Personal Data as required for compliance with all Data Protection Laws and this Agreement;

2.1.2 are informed of the confidential nature of the Received Personal Data and the relevant party's obligations under this Agreement and subject to appropriate obligations of confidentiality;

2.1.3 do not publish, disclose or divulge any of the Received Personal Data to any third party where the party subject to this obligation would not be permitted to do so;

2.1.4 are subject to (and comply with) a binding written contractual obligation to keep the Received Personal Data confidential (unless disclosure is required under UK Law);

APPENDIX 4
TRANSPARENCY ARRANGEMENTS

The Shared Personal Data is already collected through the Subject Matters' engagement with the Criminal Justice System. The analysis' legal basis for using the data is that it is covered by GMP's function to protect life and to prevent and detect crime and by MOJ's function to protect the public.

In this context, there are no additional obligations for the Disclosing Party apart from those already listed in Section 5.2. Similarly, there are no additional obligations for the Receiving Party apart from those already listed in Section 6.1.

There is an expectation that any privacy notice in use in an operational context includes a general research and analysis provision to manage expectations around the use of the data for additional purposes - this is covered in the MoJ's Transparency Toolkit. The MoJ core privacy notices can be found on gov.uk:

https://www.gov.uk/government/organisations/ministry-of-justice/about/personal-information-charter
https://www.gov.uk/government/organisations/hm-prison-and-probation-service/about/personal-information-charter
https://www.gov.uk/government/publications/hmcts-privacy-policy

The UK GDPR allows personal data to be used for additional purposes as long as it is a 'compatible' purpose – research and statistical purposes are considered a compatible purpose. There is still a requirement to be transparent about the additional purposes unless an exemption applies. The MoJ's approach is to rely on an exemption from the transparency principle where data is not collected directly from the data subject by the Data & Analysis directorate:

In accordance with the UK GDPR Article 14(5), the provisions set out in A14 (1-4) do not apply to this processing as the provision of such information would prove impossible or would involve a disproportionate effort in relation to the purpose for processing (research/statistics). The processing will be subject to appropriate safeguards to protect the interests of data subjects in accordance with Article 89(1).

APPENDIX 5
GOVERNANCE AND REVIEW

1 Contact Points

1.1 The Contact Point for the Receiving Party for issues arising under this Agreement is as follows:

[redacted]

Physical location: [redacted]

1.2 The Contact Point for the Disclosing Party for issues arising under this Agreement is as follows:

[redacted] GMP

Physical location: [redacted]

1.3 The parties have designated the Contact Points identified above, as the first contact points for third parties in relation to Data Subject Requests and Communications and any other matter relating to the Shared Personal Data. Each party's respective Contact Point shall have overall internal responsibility within their respective party for appropriately addressing and responding to Data Subject Requests and Communications within the scope of that party's obligations.

1.4 Any notice or communication that is required by this Agreement to be sent to a Contact Point shall be sent to the relevant email address of the Contact Point. Such notices and communications shall be processed within the delivery times appropriate for similar types of communication.

2 Reporting

2.1 The parties each undertake that they shall report to the other party every 6 months on:

2.1.1 the volume of Data Subject Requests (or purported Data Subject Requests) relating to Shared Personal Data from Data Subjects (or third parties on their behalf); and

2.1.2 any Communications relating to the Shared Personal Data (including any requests for disclosure of the Shared Personal Data which is required or purported to be required by applicable law), that it has received during that period.

3 Relationship between Contact Points

3.1 The Contact Points of each party shall meet, by phone if necessary, not less than once every 3 months to manage the relationship between the parties and assess:

3.1.1 the overall effectiveness of the sharing arrangements set out in this Agreement;

3.1.2 any Communications or other areas of concern;

3.1.3 whether the objectives as set out in Appendix 2 of this Agreement are being met;

3.1.4 whether each Permitted Lawful Basis and Permitted Purpose remain valid and appropriate;

3.1.5 whether the benefits as set out in Appendix 2 of this Agreement are being delivered and whether the Shared Personal Data needs to continue to be shared;

3.1.6 whether the privacy notices and arrangements under this Agreement remain appropriate;

3.1.7 the latest quality checks conducted under Appendix 2 of this Agreement (or any similar data);

3.1.8 whether the risks of the data sharing have changed; and

3.1.9 whether the technical and organisational measures as set out at Appendix 3 of this Agreement are adequate.

3.2 Following each meeting pursuant to this paragraph 3, the Contact Points shall promptly provide a joint report of their findings to the Governance Committee referred to in paragraph 6 of this Appendix 5.

4 Quality checks

Given the Shared Personal Data will be shared within two one-off data transfers and there will be no updates to these, it is not necessary to conduct periodic tests of samples of the Shared Personal Data. The Disclosing and Receiving Party are responsible for quality checks at the time of transfer only.

5 Review

5.1 The parties shall review periodically the content of this Agreement (the **Review**), which shall include confirmation:

5.1.1 that the arrangements reflect current practice and the objectives of the parties;

5.1.2 that the scope of the Permitted Purpose is still relevant and the scope for which the Shared Personal Data is being used by the Receiving Party has not been expanded without agreement of the parties;

5.1.3 that the benefits to society, as stated in Appendix 2 of this Agreement are being realised;

5.1.4 whether it would be appropriate to undertake a new data protection impact assessment;

5.1.5 whether the arrangements in this Appendix 5 are adequate and working in practice;

5.1.6 that any relevant new guidance issued by any Data Protection Supervisory Authority raised by either party during the Review has been considered as part of the Review;

5.1.7 whether the Shared Personal Data should continue to be shared under this Agreement; and

5.1.8 that the Data Subjects are still the focus of the sharing arrangement and whether their rights are being respected.

5.2 The Review shall take place at least every six months following the project's commencement.

6 Governance Committee

6.1 The Receiving Party will establish a **Governance Committee** which shall include the lead Information Asset Owner for the project at the Receiving Party, the Policy Project Lead at Deputy Director level at the Receiving Party, and Adult Protection Force Lead, Det. Supt at the Disclosing Party. The Governance Committee shall meet face to face or via an online meeting at least every twelve months.

6.2 The Governance Committee shall, at each meeting, review and consider at least:

6.2.1 the areas of assessment set out for the Contact Points at paragraph 3.1 of this Appendix 5;

6.2.2 the reports provided by each Contact Point;

6.2.3 the latest Review (as described in paragraph 5 of this Appendix 5), if any; and

6.2.4 *include any other generic governance committee discussion areas;*

APPENDIX 6
PERMITTED CONTRACTORS AND SUB-CONTRACTORS

[Insert details of contractors and sub-contractors which are Permitted Recipients (if any).]

Organisation	Permitted Recipient of:	Contact details of organisation's data protection officer or other relevant employee with primary responsibility for the relevant Shared Personal Data within the organisation
N/A	N/A	N/A

Detailed procedures for addressing Data Subject Requests and Communications

Personal data is exempt from the right of access if it is processed for a function designed to protect the public. For this project this is the case as it contributes towards "Preventing or detecting unlawful acts" and "Protecting the public".

In the rare event where a Data Subject Request can be complied with without causing prejudice to the function of the project, the Contact Points at the responsible Party will follow official processes. For the Receiving Party, this involves consulting with [redacted] and following the MOJ official protocols when responding to Freedom Of Information Requests and Data Subject Requests. For the Disclosing Party, this involves contacting [redacted]

Other detailed technical and organisational measures

The Receiving Party, the Ministry of Justice, is a Government Department and therefore has very good security provisions. All data and software is stored on the Analytical Platform, which is a cloud–based ecosystem. It has assurance for significant datasets marked OFFICIAL-SENSITIVE. It follows NCSC Cloud Security Principles, implementing features such as:

- 2 factor authentication for user sign-in
- encryption of data at rest and in transit
- fine-grained access control
- extensive tracking of user behaviour, user privilege requests/changes and data flows
- multiple levels of isolation between users and system components
- Web access firewalls
- Cloud trail and lambda upload cloudwatch log
- Data storage in S3 buckets and managing access via project access logs using 2 independent approval levels

The Receiving Party has a large Data Engineering Team that maintains the Analytical platform. A Lead Data Engineer will support this project to ensure processes are followed correctly. That person will not have access to the data.

Other arrangements

The Receiving Party has established a working group (for technical modelling decisions), which meets monthly, and a steering group (for strategic project direction and decisions), which meets once every four months. The following people at the Disclosing Party are part of the cast lists for these groups but will have no access to the Shared Personal Data:

- [redacted]

The Receiving Party also works with [redacted] within the Disclosing Party to ensure the governance around the data share is compliant with both Party's policies. They will have no access to the Shared Personal Data.

The Receiving Party plans to consult with other subject matter experts on modelling approach and operational/policy implications. Only people listed within this agreement in Appendix 1 will have access to the Shared Personal Data.