



Data Protection Impact Assessment Fairfield Independent Review

Version number: 5

Completed by: Manon Roberts

Date created: 21/01/2026

Date processing due to start: 29/01/2026

Last Review Date: 03/03/2026

Next Review Date: 01/06/2025

Senior Responsible Owner: Alex Morrell

Key definitions

Personal data – any information relating to an identified or identifiable natural person

Special category personal data – Data concerning racial or ethnic origin; political opinions; religious or philosophical beliefs; health; trade union membership; sex life or sexual orientation; genetic data; biometric data.

Processing – any operation or set of operations which is performed on personal data, such as acquisition, collection, recording, organising, structuring, storage, adaption, alteration, retrieval, consultation, use, disclosure, transfer, combination, restriction, erasure, or destruction

Controller – the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

Processor – a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Part 1: Description of the project and how personal data will be used and protected.

1. What is Fairfield Review Team's role in the project: are they the controller, joint controller, or a processor?

Consider the definitions above. Has the Review Team agreed to this in the Terms of Reference?

Use this section to name other parties involved and their controller/processor status

The Fairfield Independent Review Team will act as the sole data controller for all personal data collected as part of the public engagement activities, including the survey, written submissions, Citizens' Engagement Forums. This means the Review Team will determine the purpose and means of processing these data. *Please note that this DPIA does not cover the data gathered as part of engagement with the Metropolitan Police Service.*

Personal data under the Review Team's control includes:

- Survey responses (demographic data and views/experiences shared via multiple choice and open-text fields)
- Written submissions (any demographic data and content shared via online form)
- Citizens' engagement forums participant contact details, consent forms, demographic information, and any notes taken during engagement activities

Only the Review Team will have access to raw data collected through these engagement methods. The Review Team will use the data for analysis and reporting purposes.

Third-party processors:

- **Survey platform provider (e.g. Smart Survey):** Will act as a data processor, hosting the online survey and providing technical infrastructure under instruction from the Review Team.
- **Third-party organisations:** Will act as data processors for the purposes of referring potential participants for Citizens' Engagement Forums, as far as is possible. Personal data will be processed under the instruction of the Review Team in a manner that ensures GDPR compliance.

The Metropolitan Police Service (MPS or Met) and the Mayor's Office for Policing and Crime (MOPAC) will not have access to individual-level data, personal identifiers, or any information that could identify participants. They will only receive anonymised and aggregated findings in the final report.

No other organisations will be data controllers or processors for this project. If the Review Team determines that the use of any additional third-party services is required, this will be explicitly risk-assessed and added to this DPIA.

2. Describe the overall aims of the project.

What does the project aim to achieve?

What activities are involved and how will those aims be achieved?

Does the project help a client meet a statutory objective?

The Fairfield Independent Review is an independent review of the Metropolitan Police Service (MPS or Met), looking at what progress the service has made since Baroness Casey's Review into the standards of behaviour and internal culture of the MPS in 2023. Dr Gillian Fairfield has been appointed independent chair of the review.

The aim of the public call for evidence is to gather perspectives from Londoners on their experiences with and perceptions of the Metropolitan Police Service, to assess progress against the Casey Review recommendations from the perspective of those most affected, and to identify any gaps between the Met's stated practices and the direct experiences of London residents.

The project will involve multiple engagement activities, open to London residents or those who have lived in London, aged 18+:

1. **Online public survey** — An anonymous survey open to all London residents or those who have lived in London over the last 3 years, covering awareness of the Casey Review and Met Turnaround Plan, neighbourhood policing, perceptions of Met priorities and effectiveness, trust and confidence, perceptions of culture and change, personal experiences of crime and contact with the Met (where applicable), and overall reflections on Met progress.
2. **Written submissions** — An anonymous online form allowing London residents to share their experiences, observations or views in their own words, with optional demographic questions.
3. **Citizens' Engagement Forums** — 12 deliberative forums (one per London Basic Command Unit), each with 12–15 participants, focused on developing solutions and recommendations for Met improvement. The option for confidential one-to-one discussions will be offered alongside each forum.
4. **Final report** — Production of a comprehensive report assessing Met progress, identifying gaps between stated practices and direct experiences, and providing evidence-based recommendations.

The findings will inform the independent assessment of the Metropolitan Police Service's progress and help identify areas for continued improvement. The review

supports the public interest in police accountability and the effective delivery of policing services in London.

3. Describe the personal data that will be used during this project.

Include all the known data fields or descriptions of the type of data being requested if open ended questions.

Please indicate whether it is just personal data e.g. name, address, DOB, etc or there is expected special categories of personal data e.g. health, ethnicity, sexual orientation or sex life (see full definition above).

Will it include children's information?

How much identifiable data is likely to be used? How many individuals will be affected?

If there are different stages or elements to the project please include a description of each stage that includes the processing of personal data.

Personal data will be collected during Citizens' Engagement Forums, the survey and written submissions. The type and volume of data varies by engagement method.

Survey (anonymous):

All questions in the survey, apart from the initial eligibility question which asks if respondents live in London, are optional — participants can select 'prefer not to say' to any question they do not wish to answer. Respondents can choose to answer questions on the following:

- **Demographic information (special category data):** Age, disability, gender identity, marriage or civil partnership, pregnancy and maternity, race (including colour, nationality, ethnicity or national origin, religion or belief, sex, sexual orientation, and if they were born in the United Kingdom.
- **Location data:** London Borough where respondent lives
- **Views and experiences:** Responses to structured questions and open-text fields about crime and policing experiences, perceptions of the Met, trust and confidence, awareness of Casey Review and Turnaround Plan
- **No direct identifiers collected:** No names, email addresses or other information that could directly identify individuals

The survey aims to achieve between 1,000–5,000 completed responses.

Written submissions (anonymous):

- **Demographic information (special category data, optional):** age, disability, gender identity, marriage or civil partnership, pregnancy and maternity, race

(including colour, nationality, ethnicity or national origin), religion or belief, sex, sexual orientation, and if they were born in the United Kingdom.

- **Location data (optional):** London Borough where respondent lives
- Submission content: Free-text sharing of experiences, observations or views about crime and policing in London
- **Direct identifiers collected:** We are not asking for direct identifiers, but any names, email addresses or other information that could directly identify individuals provided by respondents will not be stored, beyond any emails sent by the respondents.

The number of written submissions is uncapped but expected to be between 50–200 submissions. The word limit will be set at 1,000.

Expression of interest form for Citizens' Engagement Forums:

- **Personal data collected:** Name, email address, phone number (optional)
- **Demographic information (special category data):** Age, sex, gender identity, marital status, pregnancy or maternity status, race, religion or belief, sexual orientation, disability status, London Borough/BCU area, and if they were born in the United Kingdom
- **Information about experiences:** Broad nature of experience they wish to discuss or interest in participating in Citizens' Engagement Forums
- **Preferences:** Accessibility requirements

Expected approximately 100–200 expressions of interest.

Citizens' Engagement Forums:

- **Personal data:** Name, contact details (email address, phone number — optional), signature on consent form
- **Demographic information (special category data):** Age, sex, gender identity, marital status, pregnancy or maternity status, race, religion or belief, sexual orientation, disability status, London Borough/BCU area, and if they were born in the United Kingdom
- **Citizens' Engagement Forums session content:** Views, opinions and reflections shared during forum discussions, responses to questions and deliberations on review topics, perspectives on Met culture, standards and progress
- **Generated data:** Facilitator notes

12 forums with c.12–15 participants each = approximately 144–180 participants.

Children’s information:

The research is designed for adults (aged 18+).

Special category data:

All engagement methods may involve collection of special category personal data (depending on what participants choose to share when questions are optional), including:

- Age
- Gender identity (this is not necessarily categorised as special category data but should be treated as such)
- Marital status
- Pregnancy or maternity status
- Race
- Religion or belief
- Sex
- Sexual orientation
- Disability status
- If they were born in the United Kingdom

Participants may also voluntarily disclose information about experiences of crime, including sensitive topics such as sexual violence, domestic abuse, hate crime, or discriminatory treatment by police. While participants are not required to share such information, the nature of the research means that some individuals may choose to do so.

Volume of identifiable data:

- Survey: 1,000–5,000 anonymous responses (no direct identifiers)
- Written submissions: 50–200 anonymous submissions (direct identifiers collected only where provided by respondents, this data will not be stored outside respondents’ emails)
- Expression of interest: 100–200 individuals providing contact details
- Citizens’ Engagement Forums: 144–180 individuals with identifiable personal data

Total individuals potentially participating: Approximately 1,200–5,500 individuals across all engagement methods, with approximately 200 individuals providing directly identifiable personal data (name, contact details).

4. Describe the source(s) of the personal data.

Will the project use existing data already held or collect new personal data directly from individuals?

From who and how will we obtain personal data? How often will we obtain it?

All personal data for this project will be collected directly from individuals who choose to participate in the engagement activities and who voluntarily share information. No existing datasets or previously collected personal data will be used.

Survey: Personal data will be collected directly from survey respondents when they complete the online survey hosted on a dedicated survey platform (Smart Survey). Respondents will enter demographic information and their views/experiences directly into the survey. Data will be collected once at the point of survey completion. The survey will be open for 8 weeks (5th March to 30th April 2026).

Written submissions: Personal data will be collected directly from individuals when they complete the written submissions form on the review website. Respondents will enter optional demographic information and their written submission directly into the online form. Data will be collected once at the point of form submission. Written submissions will be accepted throughout the engagement period (5 March to 31st July).

Expression of interest form: Personal data will be collected directly from individuals who wish to participate in Citizens' Engagement Forums, and indirectly through signposting and referrals undertaken by partner third-party organisations such as victim support services and community organisations. Where third-party organisations support referrals, they may share limited personal data with the review for the purposes of facilitating contact and participation, in line with agreed data protection arrangements. Individuals who approach the review directly will complete an online expression of interest form on the review website, providing their contact details, demographic information and information about their interest in participating (Citizens' Engagement Forums). Data will be collected once when the form is submitted. The expression of interest form will be available from 5 March to 24 April 2026.

Citizens' Engagement Forums: Initial personal data (contact details and demographic information) will be obtained either directly via the expression of interest form or indirectly through referrals conducted by specialist third-party organisations on behalf of the review. Additional personal data will be collected directly during the forum process:

- **Before the Citizens' Engagement Forum:** Participants will complete a written consent form providing their signature and confirming their consent to participate.
- **During the Citizens' Engagement Forum:** Participants will share their views, opinions and deliberations during facilitated discussions. Review team notes will be made where participants consent.

Citizens' Engagement Forums will be conducted throughout the course of the Review. One-to-one sessions will be offered alongside the forums should participants prefer to speak in this format.

Frequency of data collection:

Personal data will be collected only once per participant per engagement method, except where minimal follow-up is needed to arrange participation (e.g. confirming Citizens' Engagement Forum times).

5. What lawful basis is being relied upon to process personal data?

GDPR allows the following lawful basis for personal data: **Consent / Necessary for performance of contract / Necessary for compliance with legal obligation / In the vital interest of an individual / In performance of a public task or in the public interest / Legitimate interest of organisation.**

If special categories of personal data are being used, an additional lawful basis will be required (See GDPR Article 9).

DPO advice should be sought if unsure.

If the Fairfield Review Team is a Data Processor, then the lawful basis will be set by the Data Controller.

All personal data collected as part of this project will be processed in accordance with the Fairfield Independent Review Team's data protection policies, which comply with the Data Protection Act 2018 and the UK GDPR. The lawful basis for processing depends on the type of data and the activity undertaken.

For standard personal data (names, contact details, demographic information excluding special category data):

The Review Team will rely on two lawful bases under Article 6 of the UK GDPR:

1. **Consent (Article 6(1)(a)):** Consent will be obtained from all participants before they take part in Citizens' Engagement Forums or complete the survey or written submissions. A privacy notice will be provided for each engagement method, setting out how personal data will be used, stored and deleted. For the survey and written submissions, consent is implied by completing and submitting the form after being provided with the relevant privacy notice, and participants will be asked to actively indicate their consent through a specific tick box for the use of anonymised quotes in the final report. For Citizens' Engagement Forums, participants will receive a privacy notice and information sheet and will be asked to provide explicit, informed consent through a signed consent form and verbal confirmation at the start of the session. Specific consent will also be sought for the use of anonymised quotes in the final report.
2. **Reasons of substantial public interest (Article 6(1)(e) and Schedule 1, Part 2, Paragraph 6 of the Data Protection Act 2018):** The processing of personal data is necessary for the performance of a task carried out in the public interest. The Fairfield Independent Review has been established to assess progress at the Metropolitan Police Service following the Casey Review, which is a matter of

significant public interest relating to police accountability and the effective delivery of policing services in London.

For special category data (age, disability, gender identity, marriage or civil partnership, pregnancy and maternity, race (including colour, nationality, ethnicity or national origin, religion or belief, sex, sexual orientation, health information) **additional lawful bases under Article 9 of the UK GDPR are required:**

1. **Explicit consent (Article 9(2)(a)):** For Citizens' Engagement Forums and the optional demographic questions in the survey and written submissions, participants will be made fully aware that they may be asked to provide or may voluntarily disclose special category data. They will provide explicit agreement for the Review Team to process such information through the consent process.
2. **Reasons of substantial public interest (Article 9(2)(g) and Schedule 1, Part 2, Paragraph 6 of the Data Protection Act 2018):** Collecting special category data is necessary for reasons of substantial public interest. This research is being undertaken to assess the Metropolitan Police Service's progress on issues relating to discrimination, which is in the public good. Understanding whether different demographic groups have different experiences of and perceptions about policing is essential to assessing progress against the Casey Review recommendations, which specifically addressed institutional racism, misogyny and homophobia.

Participant information will be stored securely and separately from review team notes and analysis to ensure participants' identities cannot be linked to research outputs. This separation will ensure that while consent is recorded, the findings remain anonymous at the point of analysis and reporting.

6. Will the Fairfield Review Team be transferring, disclosing or sharing personal data to any other party?

Name any other parties involved and their role.

Include our relationship to the third party and whether we are controller or processor to each other.

Are we sharing data with accredited researchers, devolved administrations, other government departments or third party contractors to process personal data on our behalf?

The Review Team will not transfer, disclose, or share any identifiable personal data collected during this project with any other party beyond the data processor arrangements outlined below.

Third-party data processors:

Personal data will be processed by the following third parties acting as data processors under instruction from the Review Team:

1. **Third party organisations for Citizens' Engagement Forums:** Will process contact details and demographic information of potential participants during promotion and referral. This DPIA outlines steps to ensure GDPR compliance, secure handling of personal data, and deletion of data once potential participants have been referred and confirmed.
2. **Survey platform provider (Smart Survey):** Survey responses will be hosted on the survey platform temporarily during the data collection period. Smart Survey is ISO27001 accredited and GDPR compliant. The survey platform will not have access to identifiable personal data as the survey is anonymous.

Sharing of anonymised outputs:

The only outputs that will be shared externally are anonymised and aggregated findings, which will form the basis of the final report. These findings will not include any personal identifiers and will be presented in such a way that no individual participant can be identified through demographic, geographical or experiential details.

Exceptional circumstances requiring disclosure:

In very limited circumstances, the Review Team may have to share information with a relevant third party if this is needed to protect participants or others from illegal or harmful activities. This includes situations where:

- There is an immediate safeguarding concern regarding a child or vulnerable adult
- There is an immediate risk of serious harm to a participant or others
- There is a legal obligation to report suspected criminal activity (e.g. terrorism, money laundering, child abuse)

Any such disclosure will be made in accordance with safeguarding and disclosure management protocols. Where safe to do so, participant consent will be sought before sharing information. Given the review's commissioning relationship with the Met, extra care will be taken when considering any disclosure to the force itself, applying a stringent test that balances seriousness of concern, risk of harm, confidentiality requirements, legal obligations and the need to maintain independence.

7. Describe the nature of the processing including the data lifecycle of the project.

Explain how the personal data will be collected/obtained, used, stored, transferred, and deleted throughout the project. If you can, include a diagram or information flow.

Collected/Obtained:

Personal data will be collected through multiple routes:

- **Survey:** Respondents will access the survey via a link on the review website or through promotional materials. They will complete the survey directly on the survey platform (Smart Survey), entering demographic information and their responses to structured and open-text questions. No personal identifiers will be collected. Survey data will be hosted temporarily on the survey platform. All questions other than an initial screening question checking for London residency will be optional.
- **Written submissions:** Individuals will access the written submissions form via the review website. They will complete the form directly online, optionally entering demographic information and providing their written submission in free-text fields. No personal identifiers will be collected unless respondents include these in their submissions. Submissions will be stored directly on the Review Team's secure IT system.
- **Expression of interest form:** Individuals interested in participating in Citizens' Engagement Forums will complete an online form on the review website, providing their name, contact details, demographic information, information about their interest in participating and their preferences (accessibility requirements). This data will be stored directly on the Review Team's secure IT system in a secure project folder with restricted access.
- **Citizens' Engagement Forums:** Contact details obtained via expression of interest forms or on-the-day bookings (for one-to-one sessions) will be used to arrange participation in Citizens' Engagement Forums. Participants may also be referred by specialist third-party organisations, which will collect initial contact details and demographic information. Before the Citizens' Engagement Forums, participants will complete a consent form (electronically or in hard copy) providing their signature. During Citizens' Engagement Forums (conducted in groups, face-to-face, or via additional one-to-one sessions), participants will share their experiences, views and opinions.

Used:

Personal data will be used only for the specific purpose of conducting the research and producing the independent review:

- **Contact details (Citizens' Engagement Forums):** Used solely to arrange participation (scheduling forums/one-to-one sessions, sending information sheets and consent forms, confirming attendance). Not used for any other purpose.
- **Demographic information:** Used to ensure diverse participation, to enable analysis by demographic groups, and to understand whether different groups have different experiences and perceptions. Demographic data will be reported in grouped categories in the final report to prevent identification.
- **Survey responses, written submissions, Citizens' Engagement Forums notes:** Used to conduct qualitative and quantitative analysis. Analysis will be conducted using secure software (e.g. SPSS or R for survey data, Atlas.ti or NVivo for qualitative data, Excel for written submissions). Only anonymised and aggregated findings will be included in outputs shared externally.

At all stages of use, personal identifiers will be separated from research data and any facilitator notes wherever possible.

Stored:

All personal data will be stored securely:

- **Survey data:** Initially hosted on the survey platform (Smart Survey) during data collection. Once the survey closes, data will be downloaded and stored on the Review Team's secure IT system in a dedicated project folder with restricted access. The Review Team will then delete the data from the Smart Survey platform in accordance with the terms set out in the DPIA.
- **Written submissions:** Stored directly on the Review Team's secure IT system in a dedicated project folder with restricted access.
- **Expression of interest forms, Citizens' Engagement Forums contact details, consent forms:** Stored on the Review Team's secure IT system in a separate secure folder from Citizens' Engagement Forums notes. Access restricted to Review Team members who need to arrange participation.
- **Citizens' Citizens' Engagement Forums notes:** Stored on the Review Team's secure IT system separately from identifiable information.

The Review Team's IT systems use encryption, two-factor authentication, and user access controls. All storage locations are fully compliant with GDPR and the Data

Protection Act 2018. Staff are prohibited from downloading or storing personal data on personal devices. All staff receive data security training. All staff receive annual data security training.

Transferred:

Personal data will only be transferred in the following limited circumstances:

- **To data processors:** Survey responses will be temporarily hosted on Smart Survey during data collection.
- **No transfer to MPS or MOPAC:** No identifiable personal data will be transferred to the Metropolitan Police Service or MOPAC. Only anonymised and aggregated findings will be shared in the final report.

Deleted:

All personal data will be retained only as long as necessary and will be deleted within six months of the project's completion (estimated March 2027):

- **Survey data:** Deleted from survey platform once downloaded (approximately June 2026). Data stored on the Review Team's secure IT system will be deleted by the Review Team (with a witness to the deletion) six months after project completion.
- **Written submissions, contact details, Citizens' Engagement Forums notes (anonymised):** Deleted from the Review Team's secure IT system six months after project completion by the Review Team (with a witness to the deletion).

The Review Team's project manager will be responsible for ensuring that data is deleted on time, with accountability resting with the Senior Responsible Owner. Secure deletion procedures will ensure permanent removal from all systems. Deletion will be carried out manually and confirmed.

Anonymised outputs: Reports containing anonymised quotes and aggregated findings (which are not considered personal data) may be retained beyond six months for the purposes of publication and dissemination.

8. Describe the control and security measures in place to protect personal data at each stage of the data life cycle of the project?

Explain what technical (e.g. passwords, access management, etc) and organisational controls (e.g. policies, training, etc) are in place to protect each action taken using the personal data.

The Fairfield Independent Review Team has established a range of technical and organisational measures to ensure that personal data collected during this project is protected throughout its lifecycle. These controls apply at each stage of data handling, from initial collection to final deletion.

Collected/Obtained:

- **Technical controls:** All online data collection (survey, written submissions, expression of interest forms) will take place via secure, encrypted connections (HTTPS). The survey platform (Smart Survey) and the Review Team's secure IT system both use encryption in transit and at rest. Two-factor authentication is required to access the Review Team's systems. The review website will be hosted securely with appropriate security certificates.
- **Organisational controls:** Access to the survey platform back-end and project folders on the Review Team's secure IT system will be restricted to vetted members of the Review Team only. Clear privacy notices are provided for all engagement methods, explaining data processing, storage, retention and rights. Survey and submission forms will include guidance not to include personal identifiable information in free-text responses (given the anonymous nature of these methods).

Used:

- **Technical controls:** All online data collection (survey, written submissions, expression of interest forms) will take place via secure, encrypted connections (HTTPS). Smart Survey (the survey platform) and the Review Team's secure IT system both use encryption in transit and at rest. Smart Survey is ISO27001 accredited.
- **Organisational controls:** Review Team members are trained in data protection and research ethics. Clear protocols are in place for handling sensitive data, including separating identifiable information from research content. The Review Team follows data protection policies and information security standards. Only Review Team members who need access to identifiable data for specific

purposes (e.g. arranging Citizens' Engagement Forums) will have access to those data.

Stored:

- **Technical controls:** All project data is stored on the Review Team's secure IT system, which is fully compliant with GDPR and the Data Protection Act 2018. Storage includes encryption at rest and in transit, two-factor authentication, automated backups, and user access controls. Dedicated project folders are created with access restricted only to relevant members of the Review Team. Participant contact details and identifiable information are stored separately from Citizens' Engagement Forums notes to ensure anonymisation.
- **Organisational controls:** Access to project folders is regularly reviewed to ensure only current project team members have access. Staff are prohibited from downloading or storing personal data on personal devices. All staff complete annual data security training to ensure organisational awareness of security obligations. Backups are encrypted and stored securely.

Transferred:

- **Technical controls:** Transfers to data processors (survey platform, third party organisations) will use secure, encrypted methods. Processors must demonstrate GDPR compliance and appropriate technical security measures. Anonymised data will be transferred via secure, encrypted methods only.
- **Organisational controls:** Processors are required to notify the Review Team of any data breaches immediately. Regular reviews of processor compliance will be conducted.

Deleted:

- **Technical controls:** Data deletion from the Review Team's secure IT system will be carried out by the project manager, witnessed by another team member, ensuring permanent removal from all systems (including backups).
- **Organisational controls:** The project manager is responsible for ensuring data is deleted on time, with oversight from the Senior Responsible Owner. A deletion schedule will be maintained and reviewed. Deletion will be documented and confirmed. Data processors will be required to confirm deletion from their systems.

Additional security measures:

- **Privacy notices:** Clear privacy notices are provided for all engagement methods, explaining data processing, storage, retention and rights.
- **Consent procedures:** Robust consent procedures for Citizens' Engagement Forums, including written consent forms and verbal confirmation.
- **Safeguarding protocols:** Clear protocols for managing disclosures and safeguarding concerns, including referral pathways to support services and procedures for rare circumstances requiring disclosure to authorities.
- **Ethical framework:** Comprehensive ethical framework underpinned by "do no harm" principle, covering independence, confidentiality, anonymisation, disclosure management, and safeguarding.
- **Incident response:** The Review Team has incident response procedures in place for data breaches or security incidents, including immediate notification to the ICO where required and notification to affected individuals.
- **Regular reviews:** This DPIA will be reviewed regularly throughout the project and updated if risks change or new processing activities are identified.

9. Does the project involve any international data transfers? How will they be safeguarded?

Are suppliers or partners transferring or holding data in locations outside the UK/EU?

This project does not involve any international transfers of personal data. All data collected will be stored and processed within the UK and the European Economic Area, using the Review Team's secure IT systems.

The Review Team's IT systems operate entirely within GDPR-compliant infrastructure. Data storage is located within the UK and EU, ensuring no transfer of data outside these jurisdictions.

Where third-party platforms are used, such as Smart Survey (the survey platform), the Review Team has confirmed that these services provide GDPR-compliant solutions.

These platforms must:

- Encrypt data at rest and in transit
- Apply strict user access controls
- Ensure compliance with UK data protection law
- Provide contractual guarantees regarding data location

Where third-party organisations are used for referring participants, they will share only the personal data necessary to facilitate contact and participation, in line with agreed data protection arrangements and the review's privacy notices.

The Review Team does not anticipate any need to transfer data outside the UK or EU. If circumstances change, this DPIA will be updated and additional risk assessments conducted.

10. How are individuals informed about the use of their personal data? Are we being transparent?

Is there a privacy notice in place that covers the processing of personal data for this project?

Is there an information sheet for or other leaflet available regarding the project?

The Fairfield Independent Review Team is committed to ensuring that all participants are fully informed about how their personal data will be collected, used, stored, and deleted during this project. Transparency is a central principle of the research practice, and a combination of privacy notices, information sheets, consent procedures, and clear website information will be used to ensure individuals understand what participation involves.

Survey:

Transparency will be ensured through a survey privacy notice linked at the beginning of the questionnaire, before any questions are answered. This notice will:

- Explain the purpose of the review and the research
- Confirm that the survey is anonymous with no collection of personal identifiers
- Outline the categories of data being collected (demographic information, views and experiences)
- Explain how responses will be analysed and reported (in aggregate, with anonymised quotes where consent is given)
- State how long data will be retained (six months after project completion)
- Confirm that data will be used only for the purposes of this review
- Explain that the review is independent and that the Met and MOPAC will not have access to individual responses
- Provide contact details for queries

Before starting the survey, participants will be asked to confirm consent for anonymised quotes from their open-text responses to be used in the report via a tick-box.

Support services information will be provided at the end of the survey.

Written submissions:

A privacy notice will be linked at the start of the written submissions form, explaining:

- The purpose of the review and how written submissions will be used
- That submissions are anonymous with no collection of personal identifiers

- What data is being collected (optional demographic information, submission content)
- How submissions will be analysed and reported (anonymised)
- How long data will be retained (six months after project completion)
- Limits to confidentiality (circumstances where information may need to be shared)
- Guidance not to include personal identifying information in submissions
- Contact details for queries

Support services information will be provided at the end of the form.

Expression of interest form:

The expression of interest form will include links to privacy notices for Citizens' Engagement Forums explaining:

- The purpose of collecting contact details (to arrange Citizens' Engagement Forums, either directly or via third-party organisations supporting with referrals)
- What data is being collected (contact details, demographic information, interest in Citizens' Engagement Forums, accessibility requirements)
- How data will be used (filtering expressions of interest and scheduling)
- How data will be stored securely and separately from research content
- How data may be shared with third-party organisations supporting referrals (where applicable)
- How long data will be retained (six months after project completion)
- That only the Review Team will have access to personal data
- Contact details for queries

Citizens' Engagement Forums:

For Citizens' Engagement Forums, transparency will be ensured through:

During sign-up: Whether selected via the expression of interest form or referred via specialist organisations, potential participants will receive initial information about the forum and data processing, and option for one-to-one conversation. If referred by a third-party organisation, participants will be informed that contact details will be shared with the Review Team. Information about Citizens' Engagement Forums being available on the same day will also be provided.

Before the forum: All confirmed participants will be sent a participant information sheet in advance, alongside a privacy notice. This will explain:

- The purpose of the research and that the Review Team is the data controller
- What personal data will be collected (contact details, demographic information, forum session content)
- Why it is being collected (to aim for representative participation as far as possible, to capture deliberative insights)
- How it will be processed (notes with consent, analysis, anonymisation)
- How it will be stored securely
- How long it will be retained (contact details deleted within six months)
- How reporting will be anonymised (no individual participants identifiable)
- Rights in relation to withdrawal (up until data is anonymised)
- Limits to confidentiality (circumstances where information may need to be shared, and limitations of group confidentiality)
- Ground rules for respectful discussion and confidentiality
- Support services available

At the start of the Citizens' Engagement Forums: The facilitator will provide a verbal briefing covering the key points, agree ground rules including confidentiality, and answer questions. Participants will provide verbal confirmation of consent.

Consent form: Participants will complete a written consent form before the Citizens' Engagement Forum begins, confirming their understanding and consent.

Review website:

The review website (fairfieldindependentreview.org.uk) will include:

- A clear explanation of the purpose and background of the review
- Information about all engagement methods and how to participate
- Full privacy notices for each engagement method
- Information about confidentiality and anonymity, including limits
- Details about how to contact the Review Team ('talk to us' inbox)
- FAQs addressing common questions about participation and data protection
- Links to support services
- Information about the review's independence from the Met and MOPAC

Consistency and accessibility:

All privacy notices, information sheets and consent forms will:

- Use clear, accessible language avoiding jargon
- Be available in alternative formats on request (e.g. easy read, large print)
- Be consistent in content whilst tailored to each engagement method
- Be reviewed to ensure GDPR compliance

This layered approach, combining privacy notices, information sheets, verbal briefings, and consent procedures, ensures that all participants are fully informed about their rights and the handling of their personal data throughout the project.

Part 2: Consultation

It may be necessary or beneficial to seek the views of relevant stakeholders (e.g., privacy groups), to better understand their concerns and uncover previously unknown risks.

If an ethical self-assessment has been carried out, or any engagement with National Statistician's Data Ethics Advisory Committee (NSDEC) please briefly describe the outcomes here.

11. Internal Consultation:

Record your consultation with business areas relevant to the project.

Provide the name of the team/departments, the activity undertaken and the outcome of that activity.

This DPIA has been prepared by the Crest Advisory project team in consultation with the Fairfield Independent Review Team.

Consultation undertaken:

- **Fairfield Independent Review Team:** Confirmed that the description of activities and proposed controls accurately reflect how the project will be delivered.
- **Crest Advisory (as advisor):** Consultation on research methodologies, data collection approaches, and technical platforms whilst confirming that Crest will have no access to personal data or identifiable information.
- **Senior Responsible Owner (SRO):** Review of the DPIA to confirm that the approach is appropriate, risks are adequately identified and mitigated, and that the project aligns with organisational data protection standards and the review's commitment to independence and ethical conduct.
- **Data Protection Officer/specialist:** Consultation on the lawful basis for processing personal data (including special category data), the adequacy of technical and organisational controls, the appropriateness of data handling arrangements, and compliance with GDPR requirements. Confirmation that the Review Team's secure IT systems and third-party platforms (survey provider) are consistent with GDPR requirements and information security standards.
- **Ethical framework development:** A separate ethical framework has been developed for the project, covering safeguarding, disclosure management,

independence, confidentiality, and the "do no harm" principle. This framework has been integrated into the DPIA risk assessment and mitigation measures.

Outcomes:

All consulted parties confirmed that:

- The data collection methods are proportionate and necessary for the research aims
- The technical and organisational controls are adequate to protect personal data
- The ethical framework appropriately addresses safeguarding and participant wellbeing
- The approach aligns with data protection policies and the review's commitment to independence

No significant concerns were raised during internal consultation.

12. External Consultation:

Consider who you will engage with and why?

Provide the name of the stakeholder, the activity undertaken and the outcome of that activity.

If consultation is not required, explain why.

External consultation specifically for the DPIA is not required at this stage. However, it is worth noting several relevant points:

Wider stakeholder engagement:

The review involves significant engagement with external stakeholders throughout the project:

- London residents participating in the survey, written submissions, Citizens' Engagement Forums
- Third party/community organisations and victim support services helping to promote the call for evidence
- The Metropolitan Police Service and MOPAC as the subjects of the review (though not involved in data processing)

For the purposes of data protection, participants will not be consulted on the DPIA itself, but they will be fully informed about how their personal data will be collected, used,

stored, and deleted through privacy notices, information sheets, consent forms, and the review website. This ensures transparency and provides individuals with the opportunity to make an informed decision about their participation.

Support service partnerships:

Discussions are ongoing with MOPAC and victim and mental health support organisations to provide support service referral pathways for participants. These discussions include consideration of data protection requirements.

Third-party processors:

This DPIA will be shared with all third-party organisations involved in Citizens' Engagement Forums referrals before any personal data is shared, with understanding of and adherence to GDPR compliance requirements, security measures, data retention and deletion procedures, and breach notification obligations confirmed.

No requirement for ICO consultation:

Based on the risk assessment in Part 3, no residual high risks are expected following mitigation. Therefore, consultation with the Information Commissioner's Office (ICO) is not required.

Ongoing stakeholder feedback:

The 'talk to us' inbox provides ongoing opportunities for participants and stakeholders to raise questions or concerns about data protection. Where issues are raised, they will be addressed and, if necessary, this DPIA will be updated.

Part 3: Identify risks relating to processing of personal data

The identification of risks is an important part of the DPIA. Use this section to consider what risks are present in the proposed processing of personal data and use this section to record how you will minimise the identified risks.

The table below illustrates how the different combinations of likelihood and severity of harm contribute to the overall risk. To assess whether a project is high risk, you should consider the likelihood *and* the severity of impact on individuals.

Risk		SEVERITY OF HARM		
		Minimal	Significant	Severe
LIKELIHOOD OF HARM	Probable	Medium	High	High
	Possible	Low	Medium	High
	Remote	Low	Low	Medium

Use the table below to list and assess all the possible risks to individuals' data and privacy that arise from this project. Be as specific and detailed as possible. The information you have provided in answer to the above questions should help to identify those risks.

Remember that processing should be looked at from a number of angles to consider all possible risks. Consider the project's lifecycle and specific points where there may be risks, for example data collection, transmission, outputs. Add additional lines as necessary.

Risk No.	Describe the risk and potential impact on individuals	Likelihood of harm <i>Remote, possible, probable</i>	Severity of harm <i>Minimal, significant, severe</i>	Overall risk <i>Low, medium, high</i>
1	During Citizens' Engagement Forums, participants may voluntarily disclose sensitive personal data such as details of health, traumatic experiences, or direct or indirect experiences of violence, discrimination or abuse. While such disclosures may be relevant to the research, there is a risk that discussing sensitive details may cause distress, re-traumatisation, or psychological harm to participants. This could negatively impact participant wellbeing.	Possible	Significant	Medium
2	Participants in the survey or written submissions may include personal identifying information in open-text responses despite guidance not to do so (e.g. names, addresses, specific dates, unique circumstances). Because these methods are anonymous, the Review Team would not be able to contact the individual to gain consent for use of this information or to offer support if a safeguarding concern is raised. This could result in inadvertent identification or inability to respond to safeguarding issues.	Possible	Significant	Medium
3	There is a risk that participants (particularly those who have experienced crime or negative interactions with police) may be reluctant to share honest views if they are not confident that their information will	Probable	Significant	High

Risk No.	Describe the risk and potential impact on individuals	Likelihood of harm <i>Remote, possible, probable</i>	Severity of harm <i>Minimal, significant, severe</i>	Overall risk <i>Low, medium, high</i>
	remain confidential and will not be shared with the Met. This could reduce the quality and validity of the data collected, undermine the review’s credibility, and prevent the review from hearing from those most affected by policing issues.			
4	There is a risk that personal data (e.g. participant contact details, Citizens’ Engagement Forums notes) could be lost, stolen, or accessed without authorisation during collection, storage, or transfer. This could result in unauthorised disclosure of sensitive information and potential harm to participants, including loss of privacy, reputational damage, distress, or loss of trust in the review. This risk is heightened given that data includes special category data and sensitive information about experiences of crime and policing.	Possible	Severe	High
5	There is a risk that participants could be indirectly identified in the final report despite anonymisation efforts, particularly where combinations of demographic characteristics, geographical details (e.g. specific BCU areas), or unique experiences are reported. This could result in identification of individuals who shared sensitive information, potentially causing embarrassment, distress, or harm.	Possible	Significant	Medium

Risk No.	Describe the risk and potential impact on individuals	Likelihood of harm <i>Remote, possible, probable</i>	Severity of harm <i>Minimal, significant, severe</i>	Overall risk <i>Low, medium, high</i>
6	In Citizens' Engagement Forums, participants share information in a group setting. Other participants will hear what is said during the session. There is a risk that other participants may not respect confidentiality and may discuss what was said outside the session, potentially identifying individuals and breaching their privacy. This could result in participants' views or experiences being shared beyond the research context, potentially causing embarrassment, distress or harm.	Possible	Significant	Medium
7	Given the review's commissioning relationship with the Met (the subject of the review), there is a risk that the independence of the review could be perceived as compromised if personal data or findings were shared with the Met prematurely or inappropriately. This could undermine public trust in the review, discourage participation, and reduce the credibility of findings. While this is primarily a reputational/credibility risk rather than a direct data protection risk, it impacts individuals' willingness to share personal data.	Possible	Significant	Medium
8	There is a risk that safeguarding concerns may be disclosed during Citizens' Engagement Forums, or in survey/submission responses (e.g. ongoing	Possible	Severe	High

Risk No.	Describe the risk and potential impact on individuals	Likelihood of harm <i>Remote, possible, probable</i>	Severity of harm <i>Minimal, significant, severe</i>	Overall risk <i>Low, medium, high</i>
	risk to a child or vulnerable adult, serious criminal activity). If these are not identified and acted upon appropriately, individuals may come to harm. There is also a risk that inappropriate disclosure to the Met (given the review's independence and the Met's role as the subject of review) could undermine participant trust or put individuals at risk.			
9	Personal data may not be adequately protected if the processor has inadequate security measures, experiences a data breach, or does not delete data as required. This could result in unauthorised access to or retention of personal data beyond the project lifecycle.	Possible	Significant	Medium

Measures to reduce risk

Use the table below to describe all the measures taken to reduce or eliminate the risks set out in the table above.

Measures relating to High or Medium risks should be approved by the Information Asset Owner or Senior Responsible Owner when conducting their sign off.

Risk Number	Measures taken to reduce or eliminate risk	Effect on risk <i>Eliminated, reduced, or accepted</i>	Residual Risk <i>Low, medium, high</i>	Measures approved <i>Yes / No</i>
1	<p>Trauma-informed approach: At least one Review Team member present at Citizens' Engagement Forums will be trained in trauma-informed techniques. Participant information: Privacy notices and information sheets will clearly explain that participants may discuss sensitive topics and will outline support available. Consent procedures: Written and verbal consent will confirm participants understand what participation involves and their right to withdraw. During sessions: Facilitators will check in with participants throughout, offer breaks, and allow participants to pause or stop at any time. Debrief and support: All Citizens' Engagement Forums participants will be offered a debrief and provided with information about support services (e.g. Samaritans, Mind, Victim Support). Safeguarding protocols: Clear protocols for identifying and responding to distress or safeguarding concerns. No obligation to disclose: Participants will be told they do not need to share any information they are uncomfortable sharing.</p>	<i>Reduced</i>	<i>Low</i>	Yes
2	<p>Clear guidance: Survey and written submission forms will include</p>	<i>Reduced</i>	<i>Low</i>	Yes

Risk Number	Measures taken to reduce or eliminate risk	Effect on risk <i>Eliminated, reduced, or accepted</i>	Residual Risk <i>Low, medium, high</i>	Measures approved <i>Yes / No</i>
	<p>prominent guidance encouraging participants not to include personal identifying information in free-text responses, explaining this is for their protection given the anonymous nature. Monitoring: All open-text responses will be actively monitored by the project team for any identifying information or safeguarding concerns. Redaction: Any personal identifying information inadvertently included will be redacted before analysis. Safeguarding protocols: If a safeguarding concern is identified in an anonymous response, the project team will follow safeguarding protocols, which may include reporting to relevant authorities where there is immediate risk of harm, even though the individual cannot be contacted directly. The survey/submission will note that the Review Team cannot respond to individual cases due to anonymity. Review website and support services: Clear information on the website directing anyone with concerns to contact the ‘talk to us’ inbox or access support services.</p>			
3	Clear communication about independence: All participant-facing	<i>Reduced</i>	<i>Medium</i>	Yes

Risk Number	Measures taken to reduce or eliminate risk	Effect on risk <i>Eliminated, reduced, or accepted</i>	Residual Risk <i>Low, medium, high</i>	Measures approved <i>Yes / No</i>
	<p>materials will emphasise that the review is independent of the Met and MOPAC. Privacy notices will explicitly state that the Met and MOPAC will not have access to individual responses, contact details, or any identifiable data. Confidentiality assurances: Privacy notices and verbal briefings will clearly explain confidentiality protections, including how data will be anonymised, how quotes will be unattributed, and how reporting will use grouped demographic categories. Limits explained: Transparency about limits to confidentiality (safeguarding, legal obligations) so participants can make informed decisions. Separate storage: Contact details will be stored separately from research content to reinforce confidentiality. Communications strategy: Proactive communications emphasising independence and confidentiality to build public confidence.</p>			
4	<p>Secure storage: All personal data will be stored on the Review Team's secure IT system with encryption at rest and in transit, two-factor authentication, and user access controls. Access controls: Access restricted to Review Team only via</p>	<i>Reduced</i>	<i>Medium</i>	Yes

Risk Number	Measures taken to reduce or eliminate risk	Effect on risk <i>Eliminated, reduced, or accepted</i>	Residual Risk <i>Low, medium, high</i>	Measures approved <i>Yes / No</i>
	<p>dedicated folders with user permissions. Regular review of who has access. Separation of data: Identifying information stored separately from research content (notes) to ensure anonymisation. No personal devices: Review Team members prohibited from downloading or storing data on personal devices. Secure transfer: Any transfers to processors via encrypted secure file transfer only. Staff training: All Review Team members complete annual data security training. Encryption: All devices used to access data are encrypted and password-protected. Processor responsibilities: Third-party processors required to demonstrate adequate security measures and GDPR compliance. Deletion protocols: Clear deletion schedule with accountability (project manager and SRO oversight). Permanent deletion from all systems.</p>			
5	<p>Anonymisation protocols: All personal identifiers (names, specific locations, dates, unique circumstances) will be removed from notes and reporting. Participant codes applied during analysis. Demographic grouping: Where numbers are small,</p>	<i>Reduced</i>	<i>Low</i>	Yes

Risk Number	Measures taken to reduce or eliminate risk	Effect on risk <i>Eliminated, reduced, or accepted</i>	Residual Risk <i>Low, medium, high</i>	Measures approved <i>Yes / No</i>
	<p>demographic information reported in grouped categories only (e.g. "aged 25-34" not specific ages, "Black, Asian and minority ethnic" rather than specific ethnicities). Geographic aggregation: BCU-level reporting aggregated where small numbers. Specific locations not reported. Small number suppression: Small demographic or experiential categories combined or suppressed to prevent identification. Internal review: All reporting will undergo dedicated internal review to test robustness of anonymisation and check for indirect identification through combinations of characteristics. Quote checking: All quotes checked to ensure no identifying information. Quotes edited or paraphrased where necessary to protect anonymity whilst preserving meaning. Anonymised quotes only used in the final report where explicit consent was provided by the participant.</p>			
6	<p>Ground rules: At the start of each Citizens' Engagement Forum, facilitators will agree ground rules with participants, including respecting confidentiality and not discussing who said what outside the session.</p>	<i>Reduced</i>	<i>Low</i>	Yes

Risk Number	Measures taken to reduce or eliminate risk	Effect on risk <i>Eliminated, reduced, or accepted</i>	Residual Risk <i>Low, medium, high</i>	Measures approved <i>Yes / No</i>
	<p>Participant information: Information sheets will explain the group nature of Citizens' Engagement Forums and the importance of respecting confidentiality, whilst acknowledging that the Review Team cannot guarantee other participants will maintain confidentiality. Emphasis on anonymity in reporting: Explain that reporting will not identify individual participants, reducing the incentive for others to breach confidentiality.</p> <p>Facilitator management: Trained facilitators will create a respectful environment and reinforce confidentiality throughout the session.</p> <p>Consent acknowledgement: Consent forms will acknowledge participants understand the group nature and limitations of confidentiality. Small group size: Limiting Citizens' Engagement Forum size to 12-15 participants reduces the number of people who hear each contribution.</p>			
7	<p>Clear governance: Only the Review Team will act as data controller with access to personal data, explicitly excluding the Met and MOPAC from access to identifiable information.</p> <p>Privacy notices: All participant</p>	<i>Reduced</i>	<i>Low</i>	Yes

Risk Number	Measures taken to reduce or eliminate risk	Effect on risk <i>Eliminated, reduced, or accepted</i>	Residual Risk <i>Low, medium, high</i>	Measures approved <i>Yes / No</i>
	<p>materials will clearly state the Met and MOPAC will not have access to identifiable data. Independence statement: Public-facing independence statement on website and in materials. No premature sharing: Engagement findings will not be shared with the Met before the final report is published (only anonymised aggregated findings in final report). Disclosure protocols: Stringent test applied before any disclosure to the Met (e.g. safeguarding concerns), balancing risk, harm, confidentiality, legal obligations and independence. Participant consent sought where safe to do so. Communications: Proactive communications emphasising independence to build public confidence.</p>			
8	<p>Safeguarding protocols: Comprehensive safeguarding protocols in place setting out thresholds, escalation routes, and responsibilities. Staff training: All Review Team members trained in recognising safeguarding concerns and applying protocols. Support services: Partnership with MOPAC/alternative services to provide referral pathways. Information about</p>	<i>Reduced</i>	<i>Low</i>	Yes

Risk Number	Measures taken to reduce or eliminate risk	Effect on risk <i>Eliminated, reduced, or accepted</i>	Residual Risk <i>Low, medium, high</i>	Measures approved <i>Yes / No</i>
	<p>support services provided to all participants. Monitoring: Active monitoring of all open-text responses and expression of interest forms for safeguarding concerns. Disclosure management: Clear procedures for handling disclosures, applying stringent test before any disclosure to the Met (balancing seriousness, risk, confidentiality, legal obligations, independence). Where safe, seek participant consent before disclosure. Clear routes for reporting to appropriate authorities (e.g. Local Authority Safeguarding Team, police for immediate threats, not necessarily Met if safeguarding concern relates to policing). Limits explained: Privacy notices clearly explain circumstances where confidentiality may be limited (safeguarding, legal obligations). Do no harm principle: Overarching "do no harm" principle ensures participant wellbeing is prioritised.</p>			
9	<p>Processor selection: Only processors with demonstrated GDPR compliance, appropriate security measures (encryption, access controls), and good reputation will be used.</p> <p>Minimise data sharing: Only essential data shared with processors (e.g. survey platform does not receive</p>	<i>Reduced</i>	<i>Low</i>	Yes

Risk Number	Measures taken to reduce or eliminate risk	Effect on risk <i>Eliminated, reduced, or accepted</i>	Residual Risk <i>Low, medium, high</i>	Measures approved <i>Yes / No</i>
	<p>identifiers as survey is anonymous.</p> <p>Time-limited processing: Data deleted from processor systems as soon as processing is complete.</p> <p>Regular review: Processors required to notify of any breaches immediately.</p>			

Part 4: Sign off

Approved by Review Team SRO	Date	Comments

DPO Review and Recommendation (if required)	Date	Comments
N/A	N/A	N/A

Data Protection Specialist Comments (if required)	Date	Comments
N/A	N/A	No residual high risks identified following mitigation

Once signed-off you should not consider the DPIA finished. It is intended to be a living document, reviewed, amended, and signed off as the needs and parameters of the project change. Anytime a new risk is added to the DPIA, or a current risk is increased, the DPIA will need to be signed off again.

Document Revision History

Use this section to record key changes between different versions of DPIAs.

Document Version	Date	Changes
1	13/01/2026	Initial DPIA created

2	20/01/2026	Data controllers changed from Fairfield Review Team AND Crest Advisory to Fairfield Review Team only
3	21/01/2026	Interviews replaced with Citizens' Surgeries
4	10/06/2026	<p>Removed references to recordings and transcripts and confirm Otter.AI is used for notes only</p> <p>Replaced "citizens' panels" and "citizens' juries" with "citizens' engagement forums", including an option for one-to-one meetings alongside this.</p> <p>Replaced "lived experience" with "direct experience"</p> <p>Changed age eligibility from 16+ to 18+ throughout the document</p> <p>Removed all references to payment and the collection of bank details</p>
5	03/03/2026	<p>Call for evidence, public survey, expression of interest form and written submissions form launch date amended to 5th March. End date for public survey and expression of interest form amended to 30th April.</p> <p>Sex, gender identity, marital or civil partnership status, pregnancy or maternity status added as demographic information (special category data) in Expressions of Interest to participate in Citizens Engagement Forums, and in Citizens Engagement Forums</p>