

OFFICIAL

Title:	Data Protection Impact Assessment for VAWG 100 project.				
Branch / OCU:	M01				
Date created:	01/06/2023	Review date:	01/06/2025	Version:	6.0
Relevant to:	MPS VAWG Strategy				
Author:	PS REDACTED				
Collaborators:	Prof REDACTED				
GSC Classification:	Official				

This PDF may not be suitable for users of assistive technology. Please email MPSPublicationScheme@met.police.uk to request an accessible version. See our [accessibility statement](#)

OFFICIAL

Contents

1. <u>Introduction</u>	Page 3
2. <u>Lawful Processing</u>	Page 4
3. <u>Data</u>	Page 6
4. <u>Data Protection and 'Privacy Law' Assessment</u>	Page 10
5. <u>Consultations</u>	Page 20
6. <u>Risk Assessment</u>	Page 21
7. <u>Implementation of DPIA Outcomes Responsibilities</u>	Page 25
8. <u>Data Protection Impact Assessment Sign-off</u>	Page 26

Appendices

A <u>Glossary</u>	Page 27
B <u>Relevant documents</u>	Page 28

Section 1 - Introduction

This is a project aimed at combatting violence against women and girls (VAWG) by data-driven creation and updating of a prioritised list of those suspects repeatedly named by victims or witnesses as victimising women and girls. In particular, we focus on the highest harm levels across London, to inform the application of operational tactics demonstrated to be effective in preventing offences, or bringing offenders to justice and therefore restraining their potential to commit further offences

This is an additional tool in the toolkit for combatting violence against women and girls that we propose to launch as a new way to prioritise resources for the Met's proactive policing strategy. This tool will identify the most dangerous suspects harming women and girls by stacking all circa 35,000 of them in rank order - on a monthly basis - to increase our efforts to stop the most dangerous of them from causing high harm.

The top 100 VAWG suspects are thousands of times more dangerous than the vast majority of the 35,000 suspects named in a year's VAWG offence reports, yet many of them may evade intervention because their extreme danger is not recognized. While some of them have already been identified by other scanning mechanisms, the proposed approach will provide highly systematic criteria for ensuring that the most dangerous suspects receive immediate tasking.

It is hard to overstate the seriousness of the offending targeted by this method. In an early analytic result, 92% of the V100 named suspects had either murder or rape as the most serious criminal allegation against them in the past 365 days.¹ Approximately 80% of the offence reports identified the suspect based on victim or witness sources. These sources collectively accused the subjects of harming multiple victims, and many victims reported multiple separate occasions on which they had suffered repeated serious offences from the suspects.

Objective

Our vision is to prioritise our efforts against those we believe may pose the biggest risk to women & children across London, preventing harm and targeting the most violent perpetrators. We know that a small cohort of violence against women and girls (VAWG) suspects are behind a disproportionate amount of violence and harm. Our vision is that by more precise ranking and more certain tasking of those individuals, in a data-driven, pan-Met approach, we can stop further offending before it takes place and react more quickly to arrest and disrupt those posing the highest harm.

¹ To note, the VAWG 100 project requires only allegations to include offences when calculating an individual's total harm score and does not require sanctioned detections. In particular, it does not require convictions.

Section 2 - Lawful Processing

The Commissioner has set out his intention to identify the Top 100 adults who pose a danger to women and children. The aim is to create and refresh, on an ongoing basis, a prioritised list of male suspects over the age of eighteen who have committed serious violent & sex crimes against women and girls, updated monthly, for preventive police operations. This *stacking* is an initial process intended to lead to an operational *list* of nominals who are identified as currently being at large in the community. This document concerns the creation of a rank-ordered stack, from which an ongoing operational list of cases assigned for investigation will be derived.

This data will provide access to all reported crimes during a pre-defined time range (most recent 365 days) and pre-set offence parameters.

Suspects will be given a score automatically calculated by Digital Data and Technology (DDAT) programs based on the Cambridge Crime Harm Index (CCHI) value for every offence report in which the suspect is named in the preceding 365 days.

The CCHI is calculated using the sentencing guidelines for an offence. This allows for each offence to receive a weighted score that is calculated using the guidelines' starting point recommendation of the number of days of imprisonment for each offence category. Each individual suspect will receive a total CCHI score summing the individual scores across all VAWG offences alleged against them in the preceding 365 days. This is a direct application of the values created by the Sentencing Council, and does not use any Artificial Intelligence (AI) features.

The MPS has historically used CRIS as its crime reporting system. CCHI scores were therefore initially calculated by extracting CRIS data. This occurred until the Connect Wall of 28th February 2024, when we transitioned to Connect, as which point we had to extract data from Connect and CRIS simultaneously to calculate the CCHI scores. Once a period of one year has elapsed since the Connect Wall, we will use only Connect data to calculate CCHI scores.

The data (personal identifiers – name, dob, PNC ID etc alongside crime flag/code) will be extracted from CRIS for each update of the list. The stack will be updated monthly and we will store the full stack of c. 35000 nominals each month. A separate operational list, which will incorporate reviews to determine whether suspects are suitable to be tasked out by the VAWG 100 project, will be maintained until the suspect is stepped down for any reason, including (for example) incarceration. A permanent record of assigned investigations from the original stack will be maintained for audit.

Each update of the stack will look at data from the preceding 365 days, creating a rolling and changing data set in the V100 rankings, while the tasking unit will keep a permanent record of the individuals tasked out for a new investigative process triggered by the stack ranking.

From each stack only those in the top one hundred, based on total CCHI score, will be considered for possible policing action. It should be clarified here that the VAWG 100 may, and typically will, have more than one hundred suspects tasked out at any one time, as we task out cases at a faster rate than we close them. Additionally, we do not task one hundred people every month; the numbers tasked has ranged from nine at the start of the project to twenty-nine at its peak. We have averaged about fifteen people tasked per tasking meeting.

Within the Box spreadsheet for a particular stack, we store a variety of information including: name; date of birth; ethnicity; PNCID; Op Dauntless status; Op Bassano status; total CCHI score; number of offences alleged against the person. The top 100 are hived off so that the only names the tasking team sees are in the top 100.

The tasking process is as follows:

OFFICIAL

1. The MO2 VAWG team produce that month's stack and add it to the LIT V100 Box folder.
2. The VAWG HQ team and MO2 VAWG team jointly review each name to understand how that person has entered the stack, ensuring no-one is listed incorrectly due to Connect error or duplication.²
3. The VAWG HQ team then email a spreadsheet listing all new individuals to all LIT DIs.
4. The LIT DIs review the new names and then task their officers to produce intel profiles for those individuals and create a PMP. The decision of which LIT will do which profile is ordinarily based on which BCU the offender has the biggest footprint in however profile judgement can override this.
5. The LITs then add the profiles to a Box folder for their respective BCUs.
6. From the Box folder the VAWG HQ team then add the profiles to separate Box folder for that particular cohort of nominals.
7. A pre-meet, chaired by the DCS Public Protection, is held where, amongst other things, there is the opportunity to discuss the individual cases, and for the VAWG HQ team to flag any cases where there is evidence to suggest they should not be a V100 nominal.³
8. DCIs and subject matter experts (SMEs) are provided with the link to the relevant cohort Box folder.
9. A subject spreadsheet is created by the VAWG HQ team and is added to the respective cohort folder. For each nominal, this includes the name, PNCID, and a brief description of their offending. SMEs update the SME spreadsheet with any suitable tactical advice.
10. A tasking meeting is held where potential tactics against the offenders are discussed and the most appropriate BCU or OCU to deal with the offender is decided, based on where the offender lives.
11. The offender's profile remains in the relevant cohort and BCU Box folders, and is shared with the Public Protection DCI from the cohort folder and the link to the SME spreadsheet, which lists all subjects from all cohorts.
12. The Public Protection DCI for a given BCU assigns a local OIC to the investigation via a Connect Pro-active Management Plan (PMP), though this can sometimes be done via email.

Closure & Dormancy

A VAWG 100 nominal's case will be deemed closed, with no further work to be conducted on it, should any of the following criteria be met:

- Said nominal's death;
- Said nominal's deportation;
- Said nominal's receipt of a custodial sentence of at least four years;
- Said nominal's receipt of a hospital order of at least four years;
- Said nominal's permanent relocation outside of the Metropolitan Police District

A VAWG 100 nominal's case will be deemed dormant, with the PMP paused and ready to be re-activated, should any of the following criteria be met:

- Said nominal's receipt of a custodial sentence of at least six months but less than four years;
- Said nominal's receipt of a hospital order of at least six months but less than four years;
- Said nominal's lack of any VAWG 100 related convictions and any open investigations after entering the project.

² To note, some names from the previous month may still be legitimately included in the new stack if their most serious offending has not yet 'dropped off' i.e. it is still within the last 365 day period.

³ One example of this being the DCI being made aware that a prior investigation into a serious offence against the individual established their innocence or lack of guilt and without this offence their CCHI score would not be high enough to be in the VAWG 100 project.

Section 3 - Data

The V100 stacks will be limited to both male and female persons over the age of 18 who have been repeatedly named as suspects over 365 days in cases of violence against women and girls. The operational lists will only contain male suspects.

Additional criteria for an individual to be included in the stack:-

- must have at least two separate offence reports, for offences on different dates, in which they were named as suspects
- the victims in these cases must be described as females of any age over the age of 10 by either the victim or a witness, generally with date of birth indicated.

No data on other types of individuals will feed into the scoring mechanism. Of note is that while female offenders may appear in the stack, they will be extracted when producing the operational list as the aim of this project is ultimately to tackle male violence against women.

The scoring mechanism will consist solely of machine coding of each eligible offence report by the number of days of recommended imprisonment as indicated by the Cambridge Crime Harm Index⁴.

The project does not use other intelligence, opinion or factors to incorporate someone into the stack or an operational list. We can however make decisions to extract people from the stack or operational list.

List of identifiable personal data to be used:-

An attached screenshot will show the following list of identifiable data that will be deployed in the tasking process of assessing the feasibility of immediate preventive actions after the stack has been identified solely on the basis of the PNCID and related digital identifiers, including the selection criteria of VAWG offence reports with the eligible offence classifications and their assigned CCHI values based on sentencing guidelines. The following list only applies to the top 100 nominals to emerge from the digital ranking of all 35,000+ for each refreshment of the V100 stack:

Name	Required to identify individual
Date of Birth	Required to identify individual
Last known Address	Required to locate individual
PNC Number	Required to identify individual
Gender	Required to identify individual

Special Category data:-

Ethnicity	Required to identify individual, and to track Equality Impact Assessments

Criminal Offence Data

Criminal Offence Data	
-----------------------	--

⁴ See <https://academic.oup.com/policing/article/10/3/171/1753592> and <https://www.cambridge-ebp.co.uk/crime-harm-index>).

OFFICIAL

CRIS Ref Numbers	Required to identify individual and to calculate Cambridge CHI scores
Crime Flag/Code	Required to calculate CCHI score

Data Sharing With Europol

Once the most recent monthly operational list of VAWG 100 nominals has been produced, it will be shared with the MO2 Liaison Officer at Europol. A SIENA message will be sent to Europol for automated checks to be conducted on the 100 names. The handling code applied to this message will be 'H2', instructing "Not to be disseminated without the permission of the provider".

In accordance with Article 18.6 Europol Regulations, the names will be accepted for 'Determining Relevance' before being cross-checked against other countries' intelligence contributions on the Europol SOC database. In the event of no hits, the data will be deleted from the database. In the event of a match, the MO2 embed will be notified for further enquiries to be conducted with the contributing country, and the data will be retained for a further 3 years, as long as the matched contribution was within mandate under Article 18.2 ER.

In the event of a Foreign National Offender (FNO) featuring within the VAWG list, a direct bilateral SIENA (Secure Information Exchange Network Application)⁵ request will be sent to that country of origin (identified through the PNC record of that individual) asking for cross-checking against their own national police and judicial indices. This aims to identify any existing interest in that offender and may encourage collaborative working. The same H2 handling restriction will be applied to the outbound message. In the event of useful intelligence being received as a result of the request, the MO2 embed will notify the MPS team managing that offender and an assessment can be made as to its use.

The H2 restriction will ensure that the UK will be notified should another intelligence contribution match the VAWG data, but that contributor will not. Europol will not be able to use the data for any other purpose.

The ultimate purpose of this sharing is to identify whether or not any European partner agencies have interest in a given nominal, which could give rise to additional tactics for intervention in conjunction with that agency's country.

We do not require a specific memorandum of understanding for this data sharing as this will be incorporated into our broader use of SIENA.

Data Sharing With PNC

The VAWG project had originally hoped to be able to provide some form of notification to officers to make them aware when they come into contact with a VAWG 100 nominal. After consideration, the most practical means of doing this seemed to be by placing a marker on the PNC Operational Info page. On review of general PNC access, it quickly became clear that a multitude of organisations beyond the police have access to PNC, including at least one local authority⁶. This then raised concerns that statements placed on the OI page was in danger of prejudicing that person's life chances, such as their local authority seeing it and declining to provide them with housing. As such, the

⁵ SIENA is a state of the art platform that meets the communication need of EU law enforcement. It enables the swift and user friendly exchange of operational and strategic crime related information among Europol's liaison officers, analysts and experts, member states and third part countries with which Europol has cooperation / working arrangements.

⁶ Of particular concern was that if one local authority has access to PNC then surely every other local authority in the country could gain access.

OFFICIAL

worded of the notification has been selected to avoid any reference to VAWG offending or even any specific reference to the fact that the nominal is a suspect.

'Please create a Connect intel report documenting all interactions with this person, placing at the top of the intel report 'Please link this report to Connect Pro-active Management Plan with URN XYZ.' For any non-Connect forces, please submit an Intel report to MIB@met.police.uk and request that it be linked to Connect Pro-active Management Plan with URN XYZ.'

This notification was ultimately settled upon midway through the project and so there is a backlog of notification to be added, which we anticipate will be done by MO2 in bulk. Beyond this, it will be for the OIC to add on receipt of the nominal. It will on all occasions be for the OIC to remove the notification once the nominal meets the centrally agreed closure criteria.

Data Sharing With FIMS

To enhance the VAWG 100 project, each month we share the names and PNCIDs of the new nominals on the list with MO4's Central Image Identification Unit (CIIU) who work daily on the Forensic Imagery Management Service (FIMS). At present, this is shared by the VAWG HQ team via a spreadsheet in an email, though this will change once our policy on handling and retention comes into force.

Once the CIIU receive the names, they extract pictures – custody imaging held on other MPS databases – of the nominals in question and then they search FIMS for possible matches. They then submit an 'intel identification' and have a Code D compliant process of converting that identification to a 'Direct identification'

The CIIU is a small MPS team so there is no external sharing of any data, and it will not be known outside of VAWG 100 or MO4 personnel that the comparison was made. The system used by FIMS to run the comparison is subject to robust scrutiny and its own DPIA. Any FIMS identification will ultimately lead to the individual in question being regarded as a suspect and they will be subject to normal investigative actions. These actions must always be deemed justifiable, proportionate, legal, accountable and necessary by the investigator. FIMS identification by itself does not automatically trigger any police action.

Data Sharing With ANPR

To augment the project, DAC Russell agreed that we would share details of the VAWG 100 nominals' VRMs or personal data with the MO2 ANPR team who will overlay the respective ANPR hits onto the geolocation data of unsolved sexual offences, as provided via Connect. The ANPR team will analyse any travel patterns of the VAWG 100 nominals and, where appropriate, link offences and VRMs that have not previously been linked by other forensic analysis or been identified by victims or witnesses. Any links between VRMs and offences will then be shared with the respective OIC for the VAWG 100 nominal in question, and the project team itself. This data will be stored on Box with a retention period of twelve months in line with ANPR data retention, beyond which the data will be deleted. Access to the VAWG 100 nominal data will be limited to analysts and researchers from the ANPR team on a need to know basis. Access to the data will be managed by the MPS Role Based Access Control.

Data Sharing With London Regional Prison Intel Unit

The MPS London Regional Prison Intel Unit (LRPIU) are the link between policing and the eight London prisons. The LRPIU are sent a monthly email of new VAWG 100 Names who are in custody at the time of the V100 meeting; the LRPIU do not add in those who later go into custody at a later point. They also attend the monthly VAWG 100 tasking and allocation meeting. Following each VAWG 100 meeting, all subjects who are in custody are assigned a single point of contact (SPOC) from the LRPIU who will send an email providing their details and

OFFICIAL

outlining the support services they can offer. The PINS notification never outlines why a person wants to be notified of the moves of the individual in question.

A flag is added to PINS profile of all VAWG 100 nominals in prison by the LRPIU or SPOC to ensure that the LRPIU are notified by email when the nominal is released from prison, moves from one prison to another, or if there are any significant updates, which will be relayed to the OIC or relevant unit. The email only include the name of the individual, their NOMIS (prison) ID, the details of the move, and the fact that the person in question is a VAWG 100 nominal. The point at which the flag is remove is a discretionary decision by the LRPIU.

The PIU can also provide advice and support on the unwanted prisoner contact portal, which is a national unwanted prison contact services which protects victims and witness from unwanted contact in prison. This is completed via an online contact form. LRPIU also assist any ongoing investigations. Any such activity will need to be proportionate, legal, accountable, necessary and justifiable, be RIPA compliant, and be arranged by OPT forms to ensure compliance.

LRPIU store their records, including those relating to VAWG 100 nominals, in Box with their profiles, including name and date of birth, and an update sheet with all enquiries and contacts made. Only LRPIU have access to this Box folder.

Section 4 - Data Protection and Privacy Law Assessment

European Convention of Human Rights:

Article 8: Right to respect for private and family life

1. Everyone has the right to respect for their private and family life, their home and their correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The MPS is a public authority, therefore, is subject to a statutory duty under the Human Rights Act (HRA) section 6(1) not to act inconsistently with a Convention right. The relevant Convention right for the purposes of this processing is Article 8(1) of the Convention.

Article 8(1) is a qualified right and does not prohibit lawful and proportionate law enforcement activities which are necessary for the prevention or detection of crime. It is for this reason that the MPS believes that the interference with the Article 8(1) rights can be justified under Article 8(2). The purpose is the prevention and detection of crime. This falls squarely within one of the permissible bases for interference in Article 8(2), which refers specifically to the prevention of disorder or crime. For the interference to be justified it would need to be “*in accordance with the law*” and “*necessary in a democratic society*”, within the meaning of Article 8(2).

1. Does this project / initiative address a pressing social need? If so, outline it here:

Explain in detail why it is necessary to use VAWG100 for the purposes within your scope (policies for use).

As the case of Taxi-Driver rapist John Worboys shows, extremely serious offenders may commit repeated VAWG offences without prosecution over a period of many years. The number of named suspects for VAWG offences over each 365 days is in the range of 35,000—one for every Met officer. Yet the number of VAWG offences leading to prosecution and conviction is far lower. Rather than focusing on the sheer number of such cases, policing has increasingly recognized the importance of prioritizing (stacking) suspected offenders in relation to the expected severity of the crimes they are committing or may commit. That is why over 92,000 readers have accessed the Cambridge Crime Harm Index (CCHI) since it was published 7 years ago, and why Denmark, Sweden, W. Australia and New Zealand have all adopted a CCHI approach for allocating police resources. The advantage of the use of a severity metric is that it allows the MPS to focus not on each case, or each of the 35,000 suspects, as if the return on investment of scarce policing resources would be equal; it allows the MPS to prevent the *most* harm from VAWG offences with each hour of police work invested in each suspect.

What is the ‘Pressing Social Need’ – the necessity for this action in a democratic society?

The pressing social need is to reduce the rates of rape and murder of women in London. When serious VAWG offenders escape detection and prosecution, our community remains insecure and may lack confidence in the law and policing.

If you intend to process special category data in particular under Part 3 Law Enforcement Processing – why it is strictly necessary to do it this way and cognisant of alternative means which are less intrusive/risky. Strictly

necessary is a much higher level test closer to its being impossible to achieve the intended purposes unless you do it this way or is so prohibitively difficult/costly that this is the only logical solution.

The strict necessity for tracking the ethnicity of suspects, as well as victims, is to provide transparency about the distribution of police resources across ethnic groups. No matter how justified and objective this new method of allocating resources may be, it is essential to provide an ongoing account of the differential rates of policing in relation to population proportions of the suspects. While police play no role in naming the suspects in VAWG cases—which is done by victims and witnesses providing evidence—it remains strictly necessary to show that we are aware of any ethnic group disparities so that we can ensure they are strictly necessary to accomplish the protection of victims from harm.

2. Are your actions/data sharing a proportionate response to the social need this project / initiative has identified?

Explain why this is a proportionate response. To do this you apply the 4 part Bank Mellat test to frame your answer –as paraphrased below.

1 - What is your high level objective which you are seeking to accomplish by processing this way and is that objective sufficiently important to warrant the limitation of a protected right (Art 8 HRA (private life) is the obvious one but there may be others)

The high level objective is to protect vulnerable victims from extreme harm which may include but is not limited to rape, serious assault and death. This objective is so important as to curtail a protected right, that being namely the article 8 right to privacy and family life.

2 - Explain how the processing is rationally connected to the high level objective

By identifying the people named by victims and witnesses as repeatedly victimizing women and girls with the highest levels of harm, the project can cause more of those dangerous suspects to be prevented from committing future harm by their speedier incarceration for prior crimes of extreme harm.

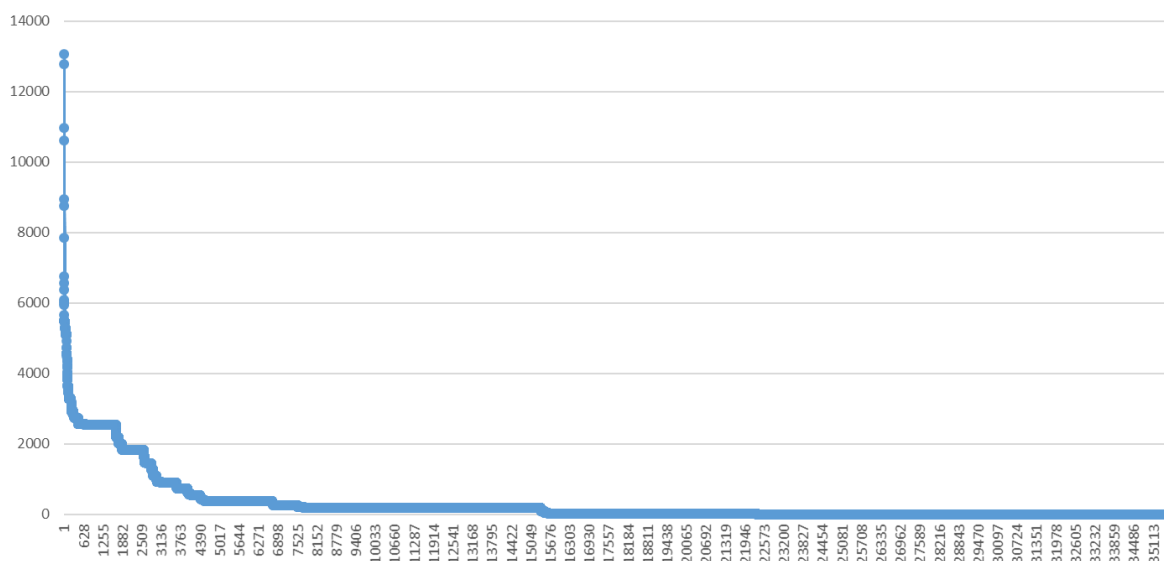
3 - What other less intrusive options have you considered?

Ranking 35000+ individuals can be characterized as an intrusive act of data processing. There are far less intrusive approaches currently used to set priorities for scarce resources, yet they have proved far less accurate and effective in identifying and preventing further offending and substantially reducing the risk of high harm to women and girls. The current strategy of investigating such crime reports reactively is also intrusive, as well as inadequate. Prosecution is often dependent on the support of victims and witnesses and this is often not forthcoming for a variety of reasons including how arduous the process of obtaining justice can appear to be. Attrition in domestic violence settings (comprising 65% of the VAWG offences analysed) is disproportionately high, and the very low and declining rates of rape conviction remains of national concern. Our aim in adopting the V100 strategy is that the ranking itself will help to increase willingness of victims and witnesses to provide evidence which is admissible in a court of law.

4 - Considering all in the round – the severity of the measure on the rights infringed and how effective the measure is at delivering the objective – explain why the step is a proportionate one.

This step is proportionate because it is limited to the most serious allegations against a small number of allegedly very harmful people. Some members of the V100 stack have 1,000 times more days of recommended imprisonment than the lower half of the full 35,000 list. At 11 days or lower, the bottom 17,500 are alleged to have committed criminal acts of harm totaling 1/1000th of the V100 cases above 10,000 days of recommended imprisonment if convicted. The graphic below, taken from a Met Blog by Lawrence Sherman (which appears in full in the annex), illustrates this enormous difference between the V100 and over half of all suspects.

Sum of CCHI Scores Across all Offences Over 365 Days for Each Suspect



Rank order of Suspected Nominals
From Highest (1) to Lowest (35113)

The V100 causes no increases in intrusion in response to any allegations of serious criminal activity. Rather, it makes all legally justified intrusiveness (from serving arrest warrants for prior crimes to covert surveillance) *even more* proportionate to the harm prevented because the harm identified is much greater by use of this method to decide which investigations to pursue with what level of resources. The basis for identifying the most harmful suspects comes almost entirely from victims of these offences, for whom CRIS data show that at least 80% of the identifications come from victims; the remaining 20% have no entry for the question of whether victims provided the information directly to the police officer in the preliminary investigation. That, in turn, is part of the proportionality of the use of victim statements, since police have a duty to investigate every one of those statements.

The high level objective is to protect vulnerable victims from extreme harm. The operational objective is to provide closer monitoring of the members of the community who are accused by other members of the community of causing extreme harm. A right for victims of crime to be protected when their suffering is reported to the police is better served by the proposal than by not proceeding with the proposal.

Data Protection Act 2018

Principle 1 (Section 35)

- (1) Processing of personal data for any of the Law enforcement purposes must be lawful and fair.
- (2) The processing of personal data for any of the law enforcement purposes 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.
- (3) In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).
- (4) The first case is where

OFFICIAL

(a) the data subject has given consent to the processing for the law enforcement as mentioned in subsection (2)(a), and (b) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(5) The second case is where

(a) the processing is strictly necessary for the law enforcement purpose,

(b) the processing meets at least one of the conditions in Schedule 8, and

(c) at the time when the processing is carried out, the controller has an appropriate policy document in place (see Section 42).

(8) In this section, “sensitive processing” means

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual's sex life or sexual orientation

Lawful

Data Protection Act 2018:

Where the processing, by its very nature, may not be considered as lawful and fair, the MPS relies on the following Sections of the Data Protection Act 2018 when processing this information:

Schedule 2, Part 1, Section 2(1)(a)(b)

2(1) “The listed GDPR provisions” and Article 34(1) and (4) of the GDPR (communication of personal data breach to the data subject) do not apply to personal data processed for any of the following purposes—

(a) the prevention or detection of crime,

(b) the apprehension or prosecution of offenders, or

(c) the assessment or collection of a tax or duty or an imposition of a similar nature,

to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c).

Schedule 2, Part 1, Section 2(2)(a)(b)

(2) Sub-paragraph (3) applies where—

(a) personal data is processed by a person (“Controller 1”) for any of the purposes mentioned in sub-paragraph (1)(a) to (c), and

(b) another person (“Controller 2”) obtains the data from Controller 1 for the purpose of discharging statutory functions and processes it for the purpose of discharging statutory functions.

The policing information is held by the MPS for the prevention or detection of crime, or the apprehension or prosecution of offenders.

Schedule 2, Part 1, Section 2(3)(a)(b)(c)(d)

OFFICIAL

(3) Controller 2 is exempt from the obligations in the following provisions of the GDPR—

(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided),

(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided),

(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers), and

(d) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in paragraphs (a) to (c),

to the same extent that Controller 1 is exempt from those obligations by virtue of sub-paragraph (1).

Schedule 1, Part 2 and Part 3 lists various conditions which, when fulfilled, allow for lawful processing of special categories of personal data and criminal convictions etc data.

Delete the Conditions which do not apply to your Project

Part 2 Substantial Public Interest Conditions

- *Statutory etc and government purposes 6(1)(2)*
- *Preventing or detecting unlawful acts Section 10(1)(2)(3);*
- *Safeguarding of children and of individuals at risk Section 18(1)(2)(3)(4).*

Part 3 Additional Conditions Relating To Criminal Convictions Etc

- *Extension of conditions in Part 2 of this Schedule referring to substantial public interest Section 36.*

Section 42 Safeguards: sensitive processing

Schedule 8, Part 3 lists conditions which are applicable for sensitive processing under Part 3 (*Law Enforcement Processing*)

sensitive processing” means—

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual’s sex life or sexual orientation.

Part 3 Conditions For Sensitive Processing Under Part 3

- *Statutory etc purposes Section 1(a)(b);*
- *Safeguarding of children and of individuals at risk Section 4(1)(2)(3)(4);*

OFFICIAL

The processing is necessary for the exercise of any functions conferred on a constable by any rule of law. The legal framework and existing body of guidance in which the MPS relies is provided by the following:

- The Data Protection Act 2018 (including Compliance Policy and Guidance)
- NPCC Authorised Professional Practice (APP)
- NPCC (2005) Guidance on NIM, NIM Guidance and NIM Codes of Practice (2005)
- APP Intelligence Management Guidance
- 2010 Guidance on the Management of Police Information
- The APP Data Protection Manual of Guidance
- MetSec Code
- MPS Information Management Support Pages
- MPS Records Management Policy (including the Retention, Review and Disposal Schedule).

Transparent –

The fact that a nominal has been selected by an automated summing of allegations against them will not be communicated to the nominal, nor to anyone else other than the analysts and investigators working on each specific case on a need-to-know basis.

Disclosure to nominals of their relative ranking could limit policing options for investigation and gathering of evidence to convict them. Unlike previous lists which were shared beyond need-to-know operational personnel, the current V100 stack will not be shared inside or outside MPS beyond case-by-case need-to-know.

Whilst those present on the list will not be directly advised of their appearance there has been extensive consultation with the public regarding the use of the VAWG100 and as such there is awareness that those who are suspected of multiple offences against women and girls are subject of this sort of action.

In the event of any and all rights requests, the Commander for Intelligence & Covert Policing will review the request and consult with Legal Services for advice on the appropriate response in relation to safeguarding of victims and potential victims. This will include any requests for right of access and rights of rectification.

Fair

The project takes in to account that whilst an individual is the suspect in an investigation this does not determine that they will necessarily be found guilty of the offence.

In the event of individuals being found not guilty of offences listed in the past 365 days, the initial tasking review team will exclude those offences. (This process will be undertaken by the Local Intelligence Teams (LITs) that assess every nominal tasked out on the basis of the initial Stack of 100. In Table Top exercises, the LITs have already identified an accused murderer whose investigation was closed because another suspect was charged with the murder. The process by which such facts are reviewed by the LITs is extensive and standard practice.)

OFFICIAL

If an exclusion of a case because a not guilty disposition or other means of clearing the accused reduces the CCHI score below the threshold level of the current stack, the nominal would then be dropped from the stack. If the nominal is dropped from the stack after any operations have already commenced, the central tasking unit would assess whether any current proactive investigations should be stepped down, or whether new intelligence would suggest a risk to victims who must be safeguarded by continued monitoring of the nominal in question.

Equality/Disproportionality

There is an Equality Impact Assessment (EIA) in progress, with detailed documentation of the relationship between victim disparity by ethnicity and suspect disparity.

Preliminary results show that non-white suspects are more likely to be named by victims and witnesses than white suspects, relative to their proportions in the London population. This is not a police-generated decision; it is the pattern of victim identification, in an estimated 80% or more of offence reports. Full details will be included in the EIA.

The only way to equalise the disparities in identification of suspects would be to discount the claims of victims in a way that would reduce police protection of victims of minority group members as suspected offenders.

In a larger view, the use of objective criteria from victim and witnesses reduces police discretion in identifying suspects with potential for implicit racial bias. The procedure proposed would create no bias against suspects, other than that created by the underlying patterns of crime and victimisation as reported to police in London.

The presence of a suspect on the V100 list is not based on any case-by-case police decisions, other than to systematically examine what victims and suspects are reporting to police. It is based on a comparative analysis of all suspects who have been named by VAWG victims.

1.	How will you tell individuals about the use of their personal data?
----	---

The MPS has a mature Information Governance Strategy and Structure in place which incorporates the requirements of the MPS to be open and transparent around the nature in which (sensitive) personal and special category data are to be processed (where possible).

The MPS has a comprehensive Privacy Notice. This notice includes full details of how a subject may exercise their right of access to their personal data.

2.	Are you content that the MPS privacy notices covers the intended processing?
----	--

	If the MPS Privacy Notice will not cover processing after seeking advice ISSU please describe in the box below the additional notice required with a link to it.
--	--

I have read the MPS Privacy Notice and I am content that it sufficiently covers the intended processing. If a notice saying the following would be added, it would make the notice even clearer: "People whose names are given to the police by other people stating that they have been victims of crime will be kept on record by the MPS, and may be subsequently analysed in relation to other alleged offenders for statistical purposes in support of resource allocation decisions by the police officers investigating such cases.

3.	Describe below whether you are relying on consent to process personal data, and how this will be collected? If obtaining consent (see explanation below) would prejudice the purpose the data is collected, what legal basis you will be using?
----	---

OFFICIAL

	<i>Note: Consent from data subjects, is not always relied upon as a legal basis to process data. This is because consent can be withdrawn by the data subject at any time. If consent is withdrawn, the MPS must delete the data and demonstrate another legal basis.</i>
We are not relying on consent to process personal data. All data within VAWG100 was initially collected for Law Enforcement purposes in line with the MPS's statutory and Common Law. Further processing and storage within VAWG100 is in line with the original purpose of its collection.	
Principle 2 (Section 36) Personal data collected for the law enforcement purpose, on any occasion must be specified, explicit and legitimate, and must not be processed in a manner that is incompatible with the purpose for which it was collected.	
	The intended processing is in line with the purposes outlined above, those listed in the Privacy Notice and our notification with the Information Commissioner's Office: Registration No: Z4888193.
1.	Have you identified potential new purposes as the scope of the project expands? If the answer to this question is 'yes', then you must seek the advice of the ISSU.
	There is no intention for the VAWG100 be utilized for a different purpose than proposed
Principle 3 (Section 37) Personal data shall be adequate, relevant and limited to the necessities of the purposes for which they are processed.	
The MPS will not process exhaustive amounts of personal information on the loose premise that it may be useful now or in the future (excessive data collection is also a breach of the DPA 35(2)(b)). This approach would be highly time and resource intensive, as well as potentially costly. If at any point, the data processed is found to be excessive to the purpose, then the processing may be ceased.	
1	Which personal data could you not use, without compromising the needs of the project?
None	
Principle 4 (Section 38) Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.	
The MPS is mindful of the potential damage and distress to the data subject, the organisation and to third parties if the data processed was inaccurate in anyway. To mitigate this, an ongoing examination of the accuracy and quality of the data must occur throughout the course of the processing. All data within VAWG100 is obtained from police systems such as Crimint, Connect (CRIS only in the initial deployment) and considered to be accurate. Data subjects have to the right to challenge the accuracy of data via Right to Rectification	
1	If the MPS is procuring new software, does it allow the data to be amended / deleted when necessary? The answer to this question must always be yes. The system should also enable the ability to note that the accuracy of information has been challenged and why.
Data can always be deleted when required.	

OFFICIAL

2	How is the MPS ensuring that personal data obtained from individuals or other organisations is accurate?
Any data obtained by the MPS from individuals is subject of checks in order to corroborate its accuracy, any information found to be inaccurate is subject of amendment	
Principle 5 (Section 39) Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose for which it is processed. The information will be retained in line with our Retention, Review and Deletion policy, document attached below: The policy can be amended to add that any stack or operating list containing V100 suspects will be deleted 365 days after it is generated.  records-manageme nt---retention-review	
1	What retention periods are suitable for the personal data the MPS will be processing?
The retention periods applied to the VAWG100 STACKS will be as short as operationally possible. There will be no archive of the refreshed STACK, as each one is intended to be as up to date as possible. The intent is to use each STACK to create a LIST for immediate decision-making, with no additional information beyond what is retained in CRIS or CONNECT or CRIMINT etc. The nominals on the LIST will be maintained until they are stepped down for reasons such as imprisonment, or one year has passed since they were identified in the Stack and placed on the LIST. These policies will be in line with MOPI groupings - https://www.college.police.uk/app/information-management/management-police-information/retention-review-and-disposal	
2	Are you procuring software that will allow the MPS to delete information in line with the corporate retention policy? (<i>The Answer to this Question must always be Yes.) If you are using current MPS software then it might not be possible to delete see guidance.</i>
Project will utilise software that allows for deletion in line with corporate retention policy	
Principle 6 (Section 40) 1. Personal data shall be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures. 2. Appropriate security includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.	
	Will be held internally on MPS systems, within a Box folder with access limited to those analysts with responsibility for producing the spreadsheet
	<u>Safeguards: Archiving:</u> Personal and special category data shall be processed where the processing is necessary for archiving purposes in the public interest
	<u>Safeguards: sensitive processing:</u> The processing of personal and special category data is reliant on the consent of the data subject and reliant on a DSA, or reliant on a condition specified in schedule 8.
Part 3 Conditions For Sensitive Processing under Schedule 8 • <i>Statutory etc purposes Section 1(a);</i>	

OFFICIAL

• <i>Protecting individual's vital interests Section 3;</i> • <i>Safeguarding of children and of individuals at risk Section 4(1)(2)(3)(4);</i>	
Miscellaneous Considerations	
1.	Complaint Handling
Complaints about the use of Personal Information in relation to this project should be handled by the MPS Data Protection Officer (DPO).	
2.	Freedom of Information Act 2000 (FoIA)
	The MPS shall demonstrate a commitment to openness and transparency regarding this processing, subject to any limitations posed by security or confidentiality requirements. The MPS is a public authority for the purposes of the FoIA 2000. This means that any information held by the MPS is accessible by the public on written request, subject to certain limited exemptions. In line with guidance from the ICO, the MPS will place this DPIA and other associated documents on our FoIA Publication Scheme, so the public can be aware of how we process personal data. The only exception to this will be the following: • Legal Advice • Commercially Sensitive material • Personal Data Pertaining to the Consultation Participants • Information which would otherwise affect the operations of the MPS and is not in the public's interest to disclose. All public requests for information should be directed to the MPS DPO.
1. Individual Rights	
GDPR Recital 1(1) the protection of natural persons in relation to the processing of personal data is a fundamental right. (2) Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.	
2.	<i>Transfers Outside the European Union (EU)</i>
	GDPR Recital 101 (3) <i>Personal data transferred from inside the EU to controllers, processors or other recipients outside international organisations (5) can only take place if, the conditions relating to the transfer of personal data are complied with by the controller or processor.</i>

Section 5 - Consultations

I have personally discussed this plan with the Met Police Ethics Board, the MOPAC Policing Ethics Panel, and the NPCC VAWG Leads, as well as a wide range of public interest groups. All meetings as of 31st July 2023 have produced positive and supportive comments, especially with regard to the protection of victims.

After the most recent meeting with the MOPAC Panel, Professor REDACTED, the Chair of the Panel authorised the inclusion of the following statement in the DPIA:

“After the meeting, the Chair of the LPEP and Commander Russell agreed to hold a further discussion to better understand some aspects of the planned operational response. In email correspondence she has noted that the LPEP was generally supportive of the approach, and expects that LPEP will be writing to us with detailed comments by mid-July, while we would still be developing our V100 operations with pilot cases.”

In an online meeting conducted on 5th June 2023 with a wide range of women’s safety groups, for example, we received encouragement to proceed as planned. These groups included

- Sister System
- Flashy Wings Ministry
- Paladin
- Kiran
- London’s Black Women Project
- Inclusion London
- Ashiana

Superintendent REDACTED has completed many in-person consultations in person since May 2023. Further online meetings are scheduled for July. Other groups and organisations consulted include the following:

EXTERNAL

- CPS, Probation Service, Youth Justice Board and court Service (represented by REDACTED, HMPPS - REDACTED, HMPPS - REDACTED, HMPPS - REDACTED, YJB - REDACTED, CPS - REDACTED, HMCTS)
- The Victim’s Voice Forum
- VAWG Reference Group
- London Borough Council members
- MOPAC – VAWG lead (REDACTED)
- Violence Reduction Unit (REDACTED)
- NPCC Lead (REDACTED)

INTERNAL

- Outreach Team (REDACTED)
- BPA (REDACTED)
- Met Detention (REDACTED)
- Met CC (REDACTED)
- Met Ethics Panel (Jon Savell)
- The Data Office
- All NPT Supts
- All PP D/Supts
- All LIT staff involved in tasking stage
- All BCU Commanders

Section 6 - Balanced Risk Assessment

OFFICIAL

Risk	Inclusion of a person on both a STACK and a LIST who is actually innocent of the very serious allegations made in order to reach the top 100 level.
Likelihood (L/M/H)	Low
Impact (L/M/H)	Moderate to high. In most cases, investigative methods will not be intrusive. Investigators may make contact with the persons who alleged the criminal activity, or may review existing evidence in the case file. In general that would not lead to high-impact intrusion such as covert surveillance or other investigations that could, in unlikely combinations of error, lead to an arrest that would lead to interviews that do not lead to charges.
Solutions/Mitigations	1. SOLUTION: Prior to each tasking meeting there is a pre-meet. Cases where a person has a serious allegation against them that has been established as malicious during the investigation will be brought to the pre-meet following enquiries with the owning Public Protection DCI. If appropriate, the DCS Public Protection will agree to remove that person from the tasking process. Additionally, if new information becomes available at the tasking meeting, there is the opportunity to descope that person at this point. 2. MITIGATION. The fact that overall, increased capacity to protect victims from further harm will contribute mitigation to the possible harm done to “false positive” cases against innocent people. Given the high probability of most V100 Suspects committing further harm that mitigation can be counterbalanced by the potential benefits to VAWG victims.—The exact probability of that mitigation will soon be calculated with increasing precision as the stacking methodology is enhanced by a Phase II improvement in identification of false positives by using a new MPS data analytic capacity to analyse much larger historic samples of convictions relative to suspect identification patterns

OFFICIAL

Risk 2

Risk	Disproportionate representation of demographic groups, leading to disproportionate enforcement
Likelihood (L/M/H)	High
Impact (L/M/H)	Low: The project is unlikely to change the demographic distribution of the offenders arrested for serious VAWG offences, since the methods will be allocated equally to suspects of all ethnicities and genders.
Solutions/Mitigations	Equality Impact Assessment in progress, testing the stacking data against court convictions of VAWG offences of the same seriousness.

OFFICIAL

Risk 3

Risk	Risks to past or future victims of V100 suspects may be increased by police interviewing victims. This could lead to suspects in previously investigated cases that did not lead to arrests or charging continuing or intensifying threats or violence by suspects against victims to discourage victim cooperation with the police—such threats being a prime reason that victims decide not to cooperate with police investigations after naming the suspect.
Likelihood (L/M/H)	Unknown. No research has been done on the risks to victims attendant to police re-opening investigations that have been inactive for a period of time, as most V100 cases will be.
Impact (L/M/H)	Unknown. If threats and intimidation occur, they may or may not be followed by further harm to the victim.
Solutions/Mitigations	The mitigation is the benefit of preventing high harm against future potential victims because the previous victims have provided evidence that leads to convictions and multi-year incapacitation of very high-harm offenders.

OFFICIAL

Risk 4

Risk	MPS data is leaked or accessed by those outside of the organisation.
Likelihood (L/M/H)	Very very low. MPS data systems are highly secure. Very few people in the MPS will have access to identities of the STACK nominals, which will be divided across 8 or more LITs. No copies of the identities of the 35,000+ will ever be generated or emailed or placed in BOX as part of the At most, an entire STACK of 100 names could be printed at a central tasking team location, carried out of police buildings, and left in a public place. Such an occurrence is not impossible, but extremely rare.
Impact (L/M/H)	If a list was found and circulated, it is extremely unlikely that it would cause direct harm to the people whose names appear on the list. The list would not, by itself, be posted in a central location such as the PNC, or a shoplifter data base, or other platforms in which there could be disclosures with adverse effects to the nominal named.
Solutions/Mitigations	The data on the full 35,000+ is never printed or placed in a stand-alone file; it is accessed for computational purposes as needed and not kept outside the central data storage environment which is heavily protected and secured.

Section 6 - Implementation of DPIA Outcomes Responsibilities

	Action to be taken	Date for completion of actions	Responsibility for action
1.	Complete EIA	August 2023	Professor REDACTED
2.	The processing will require describing on the MPS Information Asset Register (IAR) and Record of Processing Activity (ROPA)	August 2023	Commander Russell
3.	Policies; Standard Operating Procedures (SOPs); or, instructions should be produced which describe how each part of the process will work	September 2023	Commander Russell
4.	Create draft publication strategy	September 2023	Prof. REDACTED

OFFICIAL

Section 7 - Data Protection Impact Assessment Sign-off

1.	<i>Project Sponsor</i> Met Operations & Performance
	Sign Below: Name: Ben Russell Position: DAC Date: 18/09/2025
2.	<u>MPS Data Protection Officer Recommendations</u> <i>I have reviewed the DPIA and, from the information provided, am satisfied that:</i> <i>The MPS has a lawful basis for processing personal data (including special category data) in relation to the VAWG 100 project in that the processing (a) is based on law (for example, the MPS has a common law duty to protect the public, including tackling VAWG offending) and (b) is necessary for a law enforcement purpose (identifying those individuals at most serious risk of committing VAWG offences (including, for example, domestic violence/abuse and Forced Marriage)) in line with section 35 of the Data Protection Act 2018 (DPA 2018).</i> <i>To the extent that any sensitive processing is undertaken, the argument that the processing is strictly necessary for the law enforcement purpose of tackling VAWG offending has been clearly set out in the DPIA and appropriate Schedule 8 DPA 2018 conditions have been identified. The MPS also has a specific VAWG 100 appropriate policy document.</i> <i>The processing is necessary and proportionate for the reasons set out in the DPIA.</i> <i>In my view, from a data protection perspective, the most significant risk presented by the VAWG 100 is that someone might be incorrectly identified for inclusion in the list and investigated by the police. This could be seen, for example, where malicious and unfounded accusations have been made against that person in an acrimonious divorce or similar situation. In some cases, the relevant individual may be unaware of this and in others they may suffer a detriment (including, distress) by virtue of being incorrectly identified as a VAWG 100 nominal.</i> <i>I am aware that the VAWG 100 project has been live since June 2023 and that the processing of personal data described in the DPIA has been underway since then. I am also aware that a new phase of the VAWG 100 initiative is currently being considered whereby certain data may be shared with trusted third parties. Such sharing is not anticipated in this DPIA and I understand that a thorough consideration of the data protection risks and possible mitigations will be undertaken prior to any such sharing taking place. With that in mind, I recommend that an evaluation of the current VAWG 100 model is undertaken to allow us to understand whether any of the risks identified in this DPIA have materialised and what impact this has had, as well as understanding how successful the model has been in terms of addressing VAWG offending. I suggest that the</i>

OFFICIAL

	<i>results of this evaluation are fed into the risk analysis for the new data sharing initiatives and that this DPIA is updated/a new DPIA/DCAF is created to cover the third party sharing. The risks and mitigations in relation to the VAWG 100 project in general can be reconsidered at that point with the benefit of any observations and lessons learnt since the processing began.</i>
	Sign Below:
	Name: REDACTED Date: 15/09/25

OFFICIAL

Appendix A – Glossary

Term	Acronym	Description
Data Controller		Has the same meaning as in section 1(1) of the DPA, that is, the person who determines the manner in which and purposes for which Personal Data is or is to be processed either alone, jointly or in common with other persons
Data Protection Act 2018	DPA	Includes all codes of practice and subordinate legislation made under the DPA from time to time
Data Subject		Has the same meaning as in section 1(1) of the DPA being an individual who is the subject of Personal Data
Freedom of Information Act 2000	FOIA	Includes the Environmental Information Regulations 2004 and any other subordinate legislation made under FOIA from time to time as well as all codes of practice
Human Rights Act 2018	HRA	Includes all subordinate legislation made under the HRA from time to time
Information		Any information however held and includes Personal and Special Category Data, Non-personal Information and De-personalised Information. May be used interchangeably with 'Data'
Information Commissioner's Office	ICO	The independent regulator appointed by the Crown who is responsible for enforcing the provisions of the DPA and FOIA
Metropolitan Police Service	MPS	The police force for the London metropolis area (excluding the City of London)
Pseudonymous		Information that has never referred to an individual and cannot be connected to an individual.
Notification		The Data Controller's entry in the register maintained by the Information Commissioner pursuant to section 19 of the DPA
Process		Has the same meaning as in section 1(1) of the DPA and includes collecting, recording, storing, retrieving, amending or altering, disclosing, deleting, archiving and destroying Personal Data
Personal Data		Personal data is information relating to a living identified or identifiable individual

OFFICIAL

Appendix B

CCHI Scoring Mechanism

<https://academic.oup.com/policing/article/10/3/171/1753592>
<https://www.cambridge-ebp.co.uk/crime-harm-index> .



Cambridge+Crime+
Harm+Index+May+20

Appropriate Policy Document



MPS Part 3
Appropriate Policy Do

Ethics Panel



Met Ethics Final
VAWG 100 Ethics Pan