WMP Briefing Paper

Linking WMP HR data with Crime Records

(HR – Connect Dashboard for PSD)

Ethics Committee (10 May 2023)

> This project is at the proposal stage and is presented to the committee 'in principle' so that any immediate concerns can be raised.
>
> The finer details of the methodology, exact data to be used and mode of communicating the results will not be determined until after the exploratory data analysis (EDA) phase has been undertaken.
>
> Once the analyses have been completed the project will be presented to the Committee again so that the data used, methodology, findings, intention for deployment and communication plans can be examined in more detail.

Tasking

This project was tasked by Chief Superintendent Sam Ridding, Professional Standards Department (PSD) in March 2023.

Purpose

The purpose of the project is to develop a tool which allows PSD to identify where West Midlands Police (WMP) employees, volunteers, contractors and non-police personnel are recorded in crimes data, custody records, intelligence reports or incident logs.

This means that where a crime has been reported with a named victim, suspect, offender or witness, PSD can identify a potential WMP employee even where this information was not disclosed. Similarly, where an incident is reported at a home address of a WMP employee this would be identified, as would any mention in an intelligence report or time spent in custody.

The aim is to develop a Business Insight dashboard for PSD which links WMP Human Resources (HR) data with data available in Connect and ControlWorks. The data would be refreshed on a daily basis to provide a monitoring tool which complements existing vetting processes and provides assurance that the Force has the most up to date information.

The intention is that this will increase opportunities to use information available in Force systems to proactively identify any potential concerns regarding the integrity or vulnerability of employees and provide opportunities for intervention or prevention before further harm to victims occurs.

Context

The recent review by Baroness Casey[1] into the Metropolitan Police, after the abduction, rape and murder of Sarah Everard in March 2021 by a serving officer, and the conviction of another officer in January 2023 as one of the country's most prolific sexual offenders, has had a profound effect on public trust and confidence in policing nationally.

As a result of these and other cases, concerns have been raised about previous un-convicted offences committed by police employees and missed opportunities to withdraw vetting security clearance and utilise the police complaints and misconduct regime to assess whether employees are fit to serve.[2]

In January 2023 the Home Office and National Police Chiefs' Council (NPCC) announced that all police forces would check their workforce against the Police National Database (PND) to provide assurance that:

> *'where police officers, staff and volunteers have (a) been convicted of a criminal offence and / or (b) been otherwise indexed to adverse information or intelligence e.g., as a suspect, both (i) an appropriate vetting security clearance decision has been made and (ii) proper criminal and / or disciplinary investigations have been undertaken'[3]*

This process, described as the Historical Data Wash (HDW), is currently in progress. WMP has received the output of this bulk search and is currently reviewing the results. It is anticipated that it will take forces several months to determine whether they have any employee who presents as a concern and who must be subject of further enquiry and where appropriate, intervention.

This WMP Data Analytics Lab (DAL) project is proposed to enhance the national HDW by identifying any employees that have the requisite adverse information against them such that they should fail our vetting regime. This supports the Force commitment to tackle violence against women and girls (VAWG), abuse of position for sexual purpose (APSP) and to protect the most vulnerable in society. Offences committed by police employees and vulnerability linked incidents are under the national spotlight and are a significant risk to public confidence in policing. The College of Policing (CoP) Authorised Professional Practice (APP)[4] states that:

> *'A thorough and effective vetting regime is a key component in assessing an individual's integrity. It helps to reassure the public that appropriate checks are conducted on individuals in positions of trust. Vetting also identifies areas of vulnerability that could damage public confidence in a force or the wider police service.'*

However, vetting only provides a snapshot in time, whereas this tool would essentially run a daily vetting check over WMP data to identify risk associated with any employees. Crime, custody, intelligence and incident log events recorded each day will be scanned for evidence of a WMP employee footprint. This will enable PSD to investigate any matters of concern; and to identify victims who may require support but who have not disclosed their status as a WMP employee.

This tool will complement the national HDW output, which is likely to be provided as a monthly snapshot. The WMP tool will provide a daily review and the ability to identify patterns and trends over time, for

---

[1] An independent review into the standards of behaviour and internal culture of the Metropolitan Police Service, Baroness Casey (March 2023) BARONESS CASEY REVIEW Final Report (met.police.uk)

[2] Historic Data Wash of Police Workforce Nominal Records against the Police National Database (PND), Intention to Publish Strategy, National Police Chiefs' Council (NPCC) Microsoft Word - 2023_01_29 HDW Against PND (Intention to Publish) V1 Final .docx (npcc.police.uk)

[3] As above

[4] College of Policing (CoP) Authorised Professional Practice (APP) on Vetting (2021) Section 7.19 APP on Vetting (college.police.uk)

example repeat offenders, victims or locations. However, the HDW will additionally provide information about offences which may have occurred outside of the WMP Force area.

Ethical Considerations

The integrity testing of police personnel using police data in order to better deter, identify and deal with those whose conduct falls below the standards required to maintain public trust and confidence, and our legitimacy with the public underpins the reason for this data matching tool.

All police employees are subject to vetting when they apply for the role and this is periodically reviewed. Employees are under an obligation to inform WMP of any change of circumstances which includes being the subject of, or a person of interest in, a criminal investigation.[5] Therefore, this tool will bring to light new information about those employees who have failed to comply with this obligation.

Whilst not the primary objective of this approach, the tool will also highlight individuals who have been a victim of crime but did not disclose they were a WMP employee when the crime was reported (by themselves or on their behalf). PSD will consider each case and identify any potential welfare issues or vulnerability and ensure appropriate measures are put in place. For example, identifying 'repeat' victims could indicate that an employee is vulnerable to external pressure which could compromise their integrity and safeguarding measures can be implemented; or there may be welfare issues for victims of domestic abuse who could be supported by the organisation.

It is anticipated that the process will produce a number of false positive results, which has also been the case with the national HDW process. For this reason, the address field has been included in the data processing as an additional check to reduce the number of false positive matches. However, any remaining erroneous hits will be negated on a case by case basis by the additional checks conducted by the vetting team. As the project progresses, the DAL will investigate the best method for minimising the number of false positives.

The dashboard will contain sensitive information about WMP employees and therefore access will be strictly limited to a small group of named officers and staff who make up the PSD vetting team. The minimum of HR data fields will be processed (name, date of birth, address) to achieve the aim. Once the dashboard has been developed and tested, the developer will be able to remove their own access and only reinstate it if there is a need to fix an issue. It will be possible to monitor who has accessed the dashboard in the last three months.

Intended activity resulting from the project

The intention is that PSD vetting staff would access the dashboard each morning as part of their preparation for the 08:00 Threat Risk Management (TRM) meeting. This daily meeting is the opportunity to identify any risks and prioritise resources to manage them. The team will be able to flag concerns about any WMP employees that may have been involved in an event recorded within our systems.

This allows for a dynamic and continuing risk assessment against NPCC vetting standards to understand if individuals should have their requisite vetting status; or in the case of a victim whether some support or safeguarding may be required. This daily process will enable the Force to act swiftly to prevent further harm occurring and protect victims.

---

[5] College of Policing (CoP) Authorised Professional Practice (APP) on Vetting (2021) Section 7.19 APP on Vetting (college.police.uk)

Matters of concern will be manged in the normal way via PSD processes which may include, risk management plans, standards manager awareness, criminal/misconduct investigation.

The volume of names generated by the HDW suggest an internal process would produce a very small number of daily alerts and in most cases the names will already be known through business as usual processes.

Data

Data to be used:

Personal data from the following systems will be matched to enable tracking or monitoring:

Connect data:

- Crime data – roles including suspect/offender/victim/witness/additional relevant.
- PIR – named in an intelligence report
- Custody data

ControlWorks data:

- Incident logs

Oracle Fusion (HR) data:

- Personnel records

Centurion data (when data becomes available in DAL environment):

- Misconduct records

From these data sets the following personal data will be processed:

Name, date of birth, address, calls for police attendance to home address, criminal records, WMP employee identifier, WMP role and team and employment start date.

Data relating to crimes and incidents includes all records so that offences committed prior to employment are captured.

HR records are based on current employees only and will only capture the current address recorded on their record.

There is potential to link this dashboard to Centurion data in the future which would enable PSD staff to cross-reference misconduct/complaints data with Connect/ControlWorks data.

Level of analysis:

☑ Individual
    Individuals aggregated?
    ☐ Yes
    ☑ No
☐ Specific Area:
    ☐ Output Areas
    ☐ Super Output Areas - Lower
    ☐ Super Output Areas - Mid
    ☐ Wards
    ☐ Districts
☑ West Midlands
☑ Other (type of crime)

Connect and ControlWorks data will be based on events recorded within the WMP area only.
This analysis will not include any offences or other events occurring outside the WMP area (for example where an employee lives in another force area and an offence is reported to that force).

Reliability of data:

The project will undertake extensive exploratory data analysis (EDA) to identify and mitigate any data quality issues and to minimise the number of false positive results.

Sample or entirety: Entirety

Type of analysis:

☑Exploratory
☐ Explanatory
☐ Predictive
☐ Optimisation
☑ Dashboard

Proposed methodology:

To use names, dates of birth and address to match the details of any current WMP employees with nominals in WMP crime, custody, intelligence or incident log records.

Will the project eventually be automated:

☑ Yes
☐ No

The Business Insight (Qlik) dashboard will be refreshed on a daily basis.

Means of evaluation:

Not applicable – no explanatory or predictive element to this project.

ALGO-CARE considerations

As this project is at the proposal stage and is presented to the committee 'in principle' in order that any immediate concerns can be raised, the finer details of the methodology will not be determined until after the EDA. Once the analyses have been completed the projects will be presented to the Committee again so that findings and methodology can be examined in more detail.

Advisory	
If applicable, are the outputs from the algorithm to be used in an advisory capacity?	The output will be advisory. It will provide a daily automated data matching process which cannot be achieved manually and will indicate names which are worthy of further research by the PSD vetting team.
Does a human officer retain decision-making discretion?	Yes, the purpose of the tool is to provide a bulk search of police systems against the HR data. Any names highlighted by the tool would be subject to the usual checks undertaken by the vetting team as if they had been alerted by other means, for example via The Corruption Line (internal anonymous reporting tool).
Lawful	
What is the policing purpose justifying the use of the algorithm (means and ends)?	The policing purpose is to enable the Force to determine whether any of its employees have been involved in or affected by criminal activity or allegations of such, essentially enabling vetting checks against police systems to occur on a daily basis. Thus, where our systems hold information about employees who may not be maintaining high ethical and professional standards or acting with the utmost integrity, because of involvement in a criminal activity, this will be highlighted more rapidly than is currently the case. Where victim data is not being processed with the aim of investigating crime it falls under the Public Task/Public Interest purpose within the GDPR as highlighted in the DPIA.
Is the potential interference with the privacy of individuals necessary and proportionate for legitimate policing purposes?	All police employees are subject to vetting when they apply for the role and this is periodically reviewed. Employees are under obligation to inform WMP of any change of circumstances which includes being the subject of, or a person of interest in, a criminal investigation. Therefore, this tool will only bring to light new information about those employees who have failed to follow this obligation.

	The tool will also highlight individuals who have been a victim of crime but this has not been disclosed when the crime was reported (by themselves or on their behalf). This will enable the Force to identify employees who may require support or safeguarding, offering opportunities to identify and mitigate potential vulnerabilities.
In what way will the tool improve the current system and is this demonstrable?	It is not currently possible for this process to take place within WMP, hence the recent national HDW process being undertaken on behalf of forces. This locally owned process will provide an additional and more dynamic check to supplement the national HDW process which is likely to be conducted on a monthly basis in the future. Additionally, the local process will enable PSD to analyse historic data to identify any patterns and trends, for example in particular teams; or at particular career stages. This would not be possible from the HDW process which only provides a snapshot in time.
Are the data processed by the algorithm lawfully obtained, processed and retained, according to a genuine necessity with a rational connection to a policing aim?	The data are from WMP systems and are collected as part of normal operational activity and organisational employer requirements. As such data is collected in the appropriate manner and for the appropriate purposes.
Is the operation of the tool compliant with national guidance?	The analyses proposed would accord with the DCMS Data Ethics Framework 2018.[6]
Granularity	
Does the algorithm make suggestions at a sufficient level of detail given its purpose and the nature of the data processed?	The output will be at the level of the individual employee. It will describe the nature of the event (crime, custody, intelligence or incident) and the role of the employee identified (suspect, offender, victim, witness, other relevant).
Are data categorised to avoid broad-brush grouping and results and therefore issues of potential bias?	No, data will not be categorised as it will be viewed at the level of the individual.
Do the potential benefits outweigh any data quality uncertainties or gaps?	The project will include an extensive EDA element and this should highlight areas of heightened uncertainty in the data or where particular gaps exist.

---

[6] https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework

	It is acknowledged that the tool will only identify offences reported to WMP and therefore does not cover offences reported to other forces which may involve a WMP employee. However, this information gap will be addressed by the national HDW against PND. Thus, the Force should be notified of potential offences committed on other force areas on a monthly basis.
	It is acknowledged that the tool will only take account of employees' current address as recorded in the HR system.
	Despite these data gaps, the proposed tool will still be of value because there is currently no mechanism to help the Force understand which employees may have committed or been affected by criminality on a daily basis.
Is the provenance and quality of the data sufficiently sound?	The data have been gathered during the day-to-day work of WMP and will enable analyses of the type envisioned for this project.
If applicable, how often are the data to be refreshed?	Daily.
If the tool takes a precautionary approach in setting trade-offs, what are the justifications for the approach taken?	Not applicable – no explanatory or predictive element to this model.
Ownership	
Who owns the algorithm and the data analysed?	WMP would own the analyses and the data.
Does WMP need rights to access, use and amend the source code and data?	No
Are there any contractual or other restrictions which might limit accountability or evaluation?	No
How is the operation of the algorithm kept secure?	The data and the analyses are contained wholly within the WMP system and the security measures employed therein.

Challenge	
What are the post-implementation oversight and audit mechanisms, e.g. to identify any bias?	End user feedback identifying any inaccurate data would be addressed.
If the algorithm is to inform criminal justice disposals, how are individuals notified of its use?	Not applicable.
Accuracy	
Does the specification of the algorithm match the policing aim and decision policy?	Not applicable – no predictive element to this project.
Can the accuracy of the algorithm be validated periodically?	Not applicable – no predictive element to this project.
Can the percentage of false positives / negatives be justified?	Not applicable – no predictive element to this project.
How was the method chosen as opposed to other available methods?	Not applicable – no predictive element to this project.
What are the (potential) consequences of inaccurate forecasts?	Not applicable – no predictive element to this project.
Does this represent an acceptable risk?	Not applicable – no predictive element to this project.
How are the results checked for accuracy and how is historic accuracy fed back into the algorithm for the future?	Not applicable – no predictive element to this project.
How would inaccurate or out-of-date data affect the result?	Inaccurate data could lead to the PSD vetting team researching names which do not require attention.

Responsible	
Would the operation of the algorithm be considered fair?	The analyses will be fair in that each data point will be considered on its own merits.
Is the use of the algorithm transparent (taking account of the context of its use), accountable and placed under review?	The names identified by the output will be subjected to additional research and checks by the vetting team. Therefore, the results will be reviewed each day and subject to human oversight.
Would it be considered to be used in the public interest and to be ethical?	It is in the public interest to be able to provide assurance that the Force has mechanisms in place to identify employees engaged in or affected by criminal activity. This is an ethical use of personal data as WMP employees are required to behave with honesty and integrity by the Code of Ethics.
Explainable	
Is information available about the algorithm / decision-making rules and the impact of each feature?	The rules for matching the key data items of name, date of birth and address can be explained to end users.

Appendix 1: Glossary of Terms

WMP / Law Enforcement Terminology	
APP	Authorised Professional Practice
APSP	abuse of position for sexual purpose
CoP	College of Policing
DAL	Data Analytics Lab
FET	Force Executive Team
HDW	historical data wash – national checking of police workforce data against PND
HR	Human Resources
NPCC	National Police Chiefs' Council
OPCC	Office of the Police and Crime Commissioner
PCC	Police and Crime Commissioner
PND	Police National Database
PSD	Professional Standards Department
RV	recruitment vetting
TRM	Threat Risk Management meeting held daily
VAWG	violence against women and girls
WMP	West Midlands Police

Data Science Terminology	
ALGO-CARE	All projects have used the ALGO-CARE to consider ethical implications: Advisory, Lawful, Granularity, Ownership, Challenge, Accuracy, Responsible, Explainable
DCMS	Department for Digital, Culture, Media and Sport – developed the Data Science Ethical Framework.
EDA	Exploratory Data Analysis