

# Organisation Offending Checking Tool

Data Analytics Lab

September 2023

The purpose of the project is to develop a tool which allows PSD to conduct a 'daily vetting check' by identifying any West Midlands Police (WMP) employees<sup>1</sup> linked to crimes data, custody records, intelligence reports or incident logs.

---

<sup>1</sup> For the purposes of this project the term 'employee' also includes volunteer police cadet leaders and contractors who work in WMP buildings who would also be subject to vetting procedures.

# 1 Contents

1	Introduction.....	3
1.1	Context.....	4
2	Use of the tool in practice.....	6
2.1	Potential employee offenders and suspects.....	6
2.2	Identification of potential employee victims.....	7
3	Methods.....	11
3.1	Stage 1: Data processing over all employees.....	11
3.1.1	Crimes (investigations).....	11
3.1.2	Custody.....	12
3.1.3	Intelligence Reports.....	13
3.1.4	ControlWorks.....	13
3.1.5	Main Process.....	14
4	Dashboard.....	16
4.1	Initial Overview.....	16
4.2	Timelines.....	16
4.3	Crimes (investigations).....	16
4.4	Custody.....	17
4.5	Intelligence Reports.....	17
4.6	ControlWorks.....	17
5	Appendix.....	18
5.1	Glossary of Terms.....	18

## 1 Introduction

The purpose of the project is to develop a tool which allows the Professional Standards Department (PSD) to conduct a 'daily vetting check' by identifying any West Midlands Police (WMP) employees<sup>2</sup> linked to crimes data, custody records, intelligence reports or incident logs.

This means that where a crime has been reported with a named suspect, offender, victim or witness PSD can identify a potential WMP employee even where this information was not disclosed when the offence was reported. Similarly, where an incident is reported at a home address (within the West Midlands policing area) 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 dashboard would be refreshed on a daily basis to provide a monitoring tool which complements existing vetting processes with the most up to date information. 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.

This project was submitted 'in principle' to the Ethics Committee in May 2023. The committee requested more information in order to be able to offer advice (Outcome E)

- The Committee noted how important this project was and commended the Lab on proceeding with it (especially in the context of the Casey Review).
- The Committee requested greater clarity around the purpose and scope of the tool. It was proposed by the Committee that the Lab should run an internal gaming scenario in order to plan out how instances of collateral inclusion would be managed ahead of the pilot going live.
- Some members of the Committee expressed an interest in exploring possibilities around separating the offender and the victim elements of the project (although there were differing views on the Committee about this).
- Committee expressed some concern around how the searching for data of employees who may be victims is justified and requested that the Lab return to the Committee on this.
- The Committee requested further information around what parallel processes or guidance were in place (or would be in place) to support individuals identified as victims of crime (especially those who may not want police support).
- It was requested that this project would return to the Committee at the next meeting.

---

<sup>2</sup> For the purposes of this project the term 'employee' also includes volunteer police cadet leaders and contractors who work in WMP buildings who would also be subject to vetting procedures.

## 1.1 Context

Offences committed by police employees, in particular vulnerability linked offences, are under the national spotlight and are a significant risk to public confidence in policing. The recent review by Baroness Casey<sup>3</sup> 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 unconvicted 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.<sup>4</sup>

The College of Policing (CoP) Authorised Professional Practice (APP)<sup>5</sup> 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.'*

Annual vetting can only provide a snapshot in time and therefore 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'*<sup>6</sup>

This process, described as the Historical Data Wash (HDW), has been completed and WMP has had the opportunity to review the results from this bulk search of historic records.<sup>7</sup>

Moving forwards, this process will be known as **Continuous Integrity Screening (CIS)** and will provide all Forces with the details of crimes, incidents and intelligence involving our employees as a weekly update. This will be based on data from PND and will identify employees regardless of whether or not they live (or have offended) within or outside the West Midlands policing area.

To complement the national CIS weekly output, this project will provide PSD with the ability to run a daily vetting check over WMP data to identify risk associated with any

---

<sup>3</sup> 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 \(met.police.uk\)](#)

<sup>4</sup> 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 \(npcc.police.uk\)](#)

<sup>5</sup> College of Policing (CoP) Authorised Professional Practice (APP) on Vetting (2021) Section 7.19 [APP on Vetting \(college.police.uk\)](#)

<sup>6</sup> As above

<sup>7</sup> All current employee records were checked against PND records going back to 2010.

employees. Crime, custody, intelligence and incident log events recorded each day will be scanned for evidence of a WMP employee footprint.

The primary purpose is to enable rapid identification of any employee who would (subject to further in-depth checking by PSD) fail our vetting regime as a result of committing an offence. This daily process will enable the Force to act swiftly to prevent further harm occurring and protect victims in line with 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.

In addition, it will provide the ability to monitor patterns and trends over time, for example repeat offenders, victims or locations, which the CIS will not offer.

## 2 Use of the tool in practice

The PSD Vetting Gatekeeper will access the dashboard each morning as part of their preparation for the 09:00 Threat Risk Management (TRM) meeting which provides the opportunity to identify any risks and prioritise resources to manage them. The Gatekeeper will flag concerns about WMP employees who may have been involved in an event recorded within our systems in the previous 24 hours. Based on the volumes generated by the HDW process, it is assessed that the number of daily alerts will be in single figures and in most cases the names will already be known through 'business as usual' (BAU) processes.

The dashboard contains sensitive information about WMP employees and therefore access will be limited to a small group of named officers and staff from PSD, likely to be fewer than 10 people:

1. PSD Researchers who perform the daily role of Gatekeeper for all referrals coming into PSD. Therefore, if a person is flagged up on the DAL dashboard but a referral has already come in via an existing route (self-referral, email, counter corruption anonymous reporting line etc) then this referral will be treated in the usual way without further reference to the DAL dashboard.
2. Vetting Team Manager to provide guidance to Researchers when required and provide feedback of any issues to the DAL developer.
3. A member of the Counter Corruption Intelligence Team who will be able to cross reference any cases flagged on the DAL dashboard with their own stand-alone intelligence system.

Retaining both the suspect/offender and victim elements in the same dashboard reduces the number of people who need to be able to access the information. The PSD Vetting Team are the most experienced team in the Force for dealing with sensitive personal information.

### 2.1 Potential employee offenders and suspects

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 PSD of any change in their personal circumstances including being the subject of, or a person of interest in, a criminal investigation even where no further action is taken and regardless of whether it is recorded by WMP or another force. Failure to disclose this information is a breach of vetting requirements and can lead to disciplinary proceedings. This tool will bring to light new information about those employees who have failed to comply with this obligation.

A communications strategy is being developed to remind all employees of this requirement and to ensure transparency about the implementation of the weekly CIS and internal daily checking processes. This means all employees will be aware that if they fail to disclose that they are named as a suspect in a crime report, then it is likely their involvement will be exposed by these scanning processes. Publicising the use of these scanning tools is important for the protection of victims of these offenders (particularly in domestic abuse (DA) cases) so that they are not held responsible for having disclosed

the information. Legal Services and the Federation / Unions have been consulted during the development of the communications strategy.

Where the Gatekeeper assesses that a potential suspect has been identified as an employee by the dashboard and has not been reported via another route, this will be assessed by the PSD Appropriate Authority under Police Conduct Regulations and passed to a Caseworker who undertakes an investigation. This follows BAU PSD procedures. The usual outcomes will be considered depending on the case particulars, including risk management plans, standards manager awareness or criminal/misconduct investigation.

It is anticipated that the process will produce a number of false positive results<sup>8</sup>, which has also been the case with the national HDW process. The postcode has been included in the data returned, enabling PSD to undertake 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 as a result of the additional checks, for example checking previous addresses, undertaken as part of the Caseworkers' investigations. No decisions will be made about identified employees without research being conducted and information verified on source systems in order to mitigate against false positive results. Being the subject of a false positive identification would not result in any negative impact on an individual and would not be noted in their records. The reason for the incorrect identification would be investigated by the DAL and used to make improvements to the tool.

Whilst PSD investigate the potential misconduct, the investigation of the crime itself is conducted by the relevant investigation team. The PSD investigation into conduct matters runs in parallel and may never be revealed if there was no case to answer. The investigation team handling the criminal investigation will follow the Victims' Code and ensure that the right support and safeguarding measures are employed in accordance with any risk identified. Where there are cases of collateral intrusion, for example where an additional victim has been identified, normal investigative procedures would follow. Similarly, where a victim withdraws their support for the investigation (for example as can happen with domestic abuse cases), the usual policies would be followed, including consideration of a victimless prosecution if applicable. These would be managed by the team investigating the crime as BAU, rather than the PSD Caseworker investigating the conduct matters.

It has been agreed that all offences of DA and Rape and Serious Sexual Offences (RASSO) where the perpetrator is a WMP employee can be graded as High Risk, affording the victim enhanced support and safeguarding provision. The Victim's Code lead is also looking to afford victims of all crime where the perpetrator is a police employee to be afforded Priority Victim status under the code.

## **2.2 Identification of potential employee victims**

Although not the primary purpose of either the CIS or this tool, it is acknowledged that police employees who are victims of a crime, but who have chosen not to disclose this fact, will be identified by the process. The justification for including victim data in the scanning tool is that the Force has a responsibility to understand both personal and

---

<sup>8</sup> Refer to technical section of the report for information about how the potential for false positives is minimised.

organisational vulnerabilities. This includes confirming that any offences committed against our employees are investigated and ensuring that appropriate support is offered, especially where the longer-term consequences of the offence may be aggravated by the specific role the employee performs. The CIS data return will include victim data by default and once received the organisation cannot un-know what it knows and therefore has a duty of care. This internal tool will provide a daily update so potential victims can be offered support immediately, rather than waiting for the weekly CIS update. Victim data will not be for PSD to consider or action, the proposal is for this to be dealt with by the safeguarding team within the Public Protection Unit (PPU) who are responsible for processing risk assessment referrals to the multi-agency partners.

Any offence can have an impact upon victims and the presumption is that any employee who is a victim of crime will receive support from the organisation, should they wish. Often, when victims do disclose that they are an employee, support is in place and delivered through BAU processes during the crime recording phase, when the individual seeks support from their supervision or via mechanisms embedded by People and Organisational Development (POD).

It is acknowledged that some victims may prefer not to disclose that they are an employee and there is no requirement to do so for vetting purposes (except for a few specific roles). For example, an employee may not wish to disclose that they are victim in an abusive relationship or may prefer to keep their sexuality private from their colleagues. However, it can be beneficial to disclose being an employee when reporting a crime because information on the Force systems will be restricted and access limited<sup>9</sup>, thus protecting the individual's right to privacy within the organisation. As an example, an LGBTQ+ employee may not have shared details of their private life with their colleagues. However, if they report being a victim of a hate crime relating to their sexuality but do not disclose that they are a WMP employee, this personal information may become apparent to any colleague who subsequently reads the crime report as part of their duties. If the victim does disclose that they are an employee, access to that report will be restricted and their right to privacy maintained. As described above, the Force can then offer any support that may be needed, including appropriate allocation of the investigation to best offer the victim discretion and confidentiality. Therefore, the communications strategy referred to above will also encourage people to disclose that they are an employee when reporting that they are victim of a crime and will provide information about how this can be done confidentially.

Further to this, the Force has established a working group tasked with developing a policy for supporting employee victims of more serious offences, defined as:

- cases of serious sexual offences
- serious/severe injury (physical/psychological)
- where there are three or more incidents of standard risk domestic abuse (DA) in a 12-month period

It is acknowledged that these high harm offences should trigger an offer of enhanced support from the Force and partners but also that these may relate to sensitive issues in people's lives. In order to ensure a broad range of perspectives the working group

---

<sup>9</sup> PSD will be able to view the restricted log as part of their BAU processes



consists of the Force Victims' Champion, the Force Lead for MARAC<sup>10</sup> and Safeguarding as well as representatives from PSD, Unite, Legal Services, Information Management, Corporate Communications and the People and Wellbeing Team. The Police and Crime Commissioner (PCC) has been briefed and is supportive. The Superintendent fulfilling the role of Victims Champion leads on the delivery of the offer to empower victims and ensure they are included in any decisions.

In lieu of undertaking an internal gaming scenario as recommended by the Committee, the working group has had the advantage of being able to review cases from the HDW findings in order to ensure they develop a policy which is applicable for a range of likely future scenarios and which considers diverse perspectives. It was identified that in the last six years there were five employees who had been victims of serious DA/RASSO offences and had not availed themselves of support and safeguarding provision for a variety of reasons. A bespoke, discreet approach was made to these victims and an offer made utilising Independent Domestic/Sexual Violence Advisor (IDVA/ISVA) services which all five employees took up, evidencing the need to make formal provision in certain circumstances. Therefore, the working group have developed a process which aims to ensure that victims of these offences who, for whatever reason, do not feel able, empowered, or willing to seek support and have not identified themselves as a WMP employee when reporting the crime will receive a discreet offer of an enhanced package of support. This builds upon and formalises a scheme already in existence.

The enhanced offer will involve details of any such victims being passed to the Force Safeguarding Lead who will make discreet contact and offer a support package via an IDVA/ISVA. It is usual for victims to be referred to their local advisor who can signpost to specialist support services in a victim's local area. However, in the case of WMP employees, an offer will be made to refer to an alternative IDVA/ISVA to provide an additional layer of anonymity. Once a victim has been referred to the Force Safeguarding Lead, the Force has no further knowledge of whether the referral was acted upon and what further support services may have been utilised. With the support of the independent advisor or other specialist services, the victim is empowered to make their own decision about whether to disclose information to their line manager or other internal support mechanisms via occupational health. Any such support would fall within medical confidentiality rules and would not be disclosed unless desired by the victim.

Corporate Communications will also publicise this amendment to our process to reassure victims that their case will be handled sensitively and confidentially and in a manner which empowers them to determine how they want to proceed. This includes:

- ensuring that the offer includes safeguarding the individual and any wider affected parties
- taking into consideration any potential impact on the individual's capability and need for adapted work support with the necessary well-being support being implemented
- the involvement where necessary of line managers and/or senior team leaders

Therefore, the fact that an employee is a victim of crime will not be shared without prior consent unless there are aggravating factors, such as the offence being linked to serious

---

<sup>10</sup> Multi Agency Risk Assessment Conference

organised criminality, or a victim performing a role which may reinforce their own experiences of trauma.

The groups represented by legal, the Federation and Unions are all unanimously supportive of this process put in place for victims identified by the tool.

### 3 Methods

This project requires the use of data from across multiple systems, which needs to be processed and joined before it can be inputted into the Business Insight dashboard. All data used in the project is from the totality of data on Oracle Fusion and operational data held within Connect (Investigations, Custody and Intelligence Reports) and Control Works for active employees. It is expected to be updated every morning in order for PSD to assess any concerns recorded overnight.

The data sources used in this project are:

Dataset	Source	Details
Records of Contact (RoC) and Incidents	ControlWorks	Incident details, people recorded on the incident and their involvement
Crimes and the resulting investigations	Connect	Investigation details, role in crime, outcomes
Custody records	Connect	Arrest details, outcome of custody
Intelligence reports	Connect	Report details, people recorded on the report and their involvement
Person	Fusion	Employee details
Assignments	Fusion	Current employee assignment details
Address	Fusion	Current employee address details

#### 3.1 Stage 1: Data processing over all employees

Firstly, all current employees are mapped to operational systems. The mapping is based on the name and date of birth of employees and nominals on the operational systems. Where matches are found those employees are then taken forward to be fully assessed against the operational datasets by PSD.

##### 3.1.1 Crimes (investigations)

The first main system used is Connect Investigations data. All investigations recorded that are not offences recorded on duty are assessed and linked back to the role the employee had (e.g suspect, victim, other), for each unique identifier, totals are calculated for:

<b>Employees on a Crime</b>	A count of the number of employees where the individual is listed on a crime
<b>Linked Crimes/Total Offence</b>	A count of the number of crimes an employee is listed on

<b>Total Recorded Crime</b>	A count of the number of crimes an employee is listed on that is classed as a recorded crime
<b>Total Non-Crime</b>	A count of the number of crimes an employee is listed on that is classed as a non-crime
<b>Employee Suspect on a Crime</b>	A count of the number of employees where the individual is listed on a crime as a suspect
<b>Linked Crimes (Suspect)/ Suspect Flag</b>	A count of the number of crimes an employee is listed on as a suspect
<b>Employee Victim on a Crime</b>	A count of the number of employees where the individual is listed on a crime as a victim
<b>Linked Crimes (Victim) / Victim Flag</b>	A count of the number of crimes an employee is listed on as a victim
<b>Employee Witness on a Crime</b>	A count of the number of employees where the individual is listed on a crime as a witness
<b>Linked Crimes (Witness) / Witness Flag</b>	A count of the number of crimes an employee is listed on as a witness
<b>Employee Other on a Crime</b>	A count of the number of employees where the individual is listed on a crime as other
<b>Linked Crimes (Other) / Other Flag</b>	A count of the number of crimes an employee is listed on as other
<b>New Crimes Last 24 Hrs</b>	A count of the number of crimes flagged in the last 24 hours as linked to a current employee
<b>New Crimes Last 72 Hrs</b>	A count of the number of crimes flagged in the last 72 hours as linked to a current employee this is to pick up any crimes flagged over weekends and bank holidays
<b>Crime Interval</b>	The interval of time between the latest crime and the hire date to ensure that any crimes flagged before an individual was hired are not used as those will have been picked up by standard vetting
<b>VAWG Offences</b>	A count of the number of crimes an employee is listed on that are classed as VAWG

### 3.1.2 Custody

The second main system used is Connect Custody data. All arrests are assessed and linked back to the unique identifier, totals are calculated for:

<b>Employees on a Custody Record</b>	A count of the number of employees where the individual is listed on an arrest record
<b>Total Custody Records</b>	A count of the number of arrests an employee is listed on
<b>New Arrests Last 24 Hrs</b>	A count of the number of arrests flagged in the last 24 hours as linked to a current employee

<b>New Arrests Last 72 Hrs</b>	A count of the number of arrests flagged in the last 72 hours as linked to a current employee this is to pick up any arrests flagged over weekends and bank holidays
<b>Arrest Interval</b>	The interval of time between the latest arrest and the hire date to ensure that any arrests flagged before an individual was hired are not used as those will have been picked up by standard vetting

### 3.1.3 Intelligence Reports

The third main system used is Connect Intelligence data. All intelligence reports are assessed and linked back to the unique identifier, totals are calculated for:

<b>Employees on an Intelligence Report</b>	A count of the number of employees where the individual is listed on an intelligence report
<b>Total Intelligence Records</b>	A count of the number of intelligence reports an employee is listed on
<b>New Intel Reports Last 24 Hrs</b>	A count of the number of intelligence reports flagged in the last 24 hours as linked to a current employee
<b>New Intel Reports Last 72 Hrs</b>	A count of the number of arrests flagged in the last 72 hours as linked to a current employee this is to pick up any arrests flagged over weekends and bank holidays
<b>Report Interval</b>	The interval of time between the latest arrest and the hire date to ensure that any intelligence reports flagged before an individual was hired are not used as those will have been picked up by standard vetting

### 3.1.4 ControlWorks

The last main system used is ControlWorks (CW) data. All command and control RoCs and Incidents are assessed and linked back to the unique identifier, for originator and person records. The data is manually inputted and not all RoCs and Incidents have an Originator and a Person record. Data may be included where an employee is calling on behalf of someone else or reporting something whilst off duty; such returns will be subject to checking by PSD. Totals are calculated for:

<b>Employees on a CW Incident</b>	A count of the number of employees where the individual is listed on a CW Incident
<b>Total CW Incidents</b>	A count of the number of CW Incidents an employee is listed on

<b>New CW Incidents Last 24 Hrs</b>	A count of the number of CW Incidents flagged in the last 24 hours as linked to a current employee
<b>New CW Incidents Last 72 Hrs</b>	A count of the number of CW Incidents flagged in the last 72 hours as linked to a current employee this is to pick up any CW Incidents flagged over weekends and bank holidays
<b>CW Incident Interval</b>	The interval of time between the latest arrest and the hire date to ensure that any CW Incidents flagged before an individual was hired are not used as those will have been picked up by standard vetting

### 3.1.5 Main Process

For each of the employees identified as potentially linked to an investigation, arrest, intelligence report or control works incident or RoC, detailed information is extracted and formatted to display on the Business Insights dashboard. This is an iterative process carried out one by one for each employee.

1. For the selected employee, all potential versions of the employee on our systems are gathered (some people have the same ID but different versions of spellings of their names). Lists of all possible forename, surname, date of birth and PNC<sup>11</sup> ID are created, these are later used within other queries to search for the selected individual.
2. Investigations: details of each investigation that the selected individual plays a role in, summarising the role the individual played, the harm score<sup>12</sup> of the individual and the home address of the individual and incident location. This allows summarisation of
  - a. Number of investigation locations at each address
  - b. Number of investigations for each role in crime (suspect / victim / witness / other).
  - c. Outcome of each investigation
  - d. For investigations where the selected individual is the offender or suspect, establish the relationship of them to the victim.
  - e. For investigations where the selected individual is the victim, establish the relationship of them to the offender or suspect.
3. Custody: details of the number of custody records, for the selected employee.
  - a. Total number of arrests associated with the selected employee.
4. Intelligence Reports: details of the number of intelligence reports, for the selected employee.
  - a. Total number of reports associated with the selected employee.

---

<sup>11</sup> Police National Computer

<sup>12</sup> Harm in this instance is the RFG; recency, frequency and gravity whereby gravity is based on the Cambridge Crime Harm Index.

5. ControlWorks: details of every ControlWorks incident or RoC where the selected employee is either the originator of the call, or the subject of the call.
  - a. Total number of CW logs associated with the selected employee.
  - b. Count of number of incidents/RoCs created.
  - c. For all incidents, summary of incident.

## 4 Dashboard

The dashboard consists of six pages – the Initial Overview, Timelines, Crimes, Custody, Reports, ControlWorks pages, the contents and usage are described below. The usage of direct links to source systems also ensures that only the minimum necessary information is displayed in the dashboard.

### 4.1 Initial Overview

The initial overview page of the dashboard shows the various total counts of matches under the different systems' elements, highlighting the key measures from each of the datasets.

**Investigations counts:** Employees on a Crime, Total Offences, Total Recorded Crime, Total Non-Crime, Suspect Flag, Victim Flag, Witness Flag and Other Flag, New Crimes Last 24 Hrs, New Crimes Last 72 Hrs.

**Custody counts:** Employees on a Custody Record, Total Custody Records, New Arrests Last 24 Hrs, New Arrests Last 72 Hrs.

**Intelligence Report counts:** Employees on an Intelligence Report, Total Intelligence Reports, New Reports Last 24 Hrs, New Reports Last 72 Hrs.

**Control Works counts:** Employees on an CW Incident, Total CW Incidents, New CW Incidents Last 24 Hrs, New CW Incidents Last 72 Hrs.

The data table also includes the following measures and information, hire date so PSD can determine if all the instances the employee is potentially linked to were before employment or if any have occurred whilst employed, to assist with this the table holds yes/no data for each of the datasets to indicate if an event has occurred after employment began.

The filters allow for breakdowns of the sources by source dimensions.

### 4.2 Timelines

The timelines page of the dashboard shows a number of time series charts, bar charts and pivot tables highlighting the total count from each of the datasets, as well a set of filters for each dataset.

### 4.3 Crimes (investigations)

The crimes page of the dashboard shows the total counts from the initial overview page for investigations, text boxes that display investigation details and links to source systems only when an investigation is selected. The tables highlight the details of employees linked to investigations as well as a set of filters for each dataset.



There is an additional table that shows who the officer in charge of the investigation is should PSD which to contact them for more details to make a more informed decision on next steps if any.

#### **4.4 Custody**

The custody page of the dashboard shows the total counts from the initial overview page for custody. The tables highlight the details of employees linked to arrests as well as a set of filters for each dataset.

#### **4.5 Intelligence Reports**

The intelligence reports page of the dashboard highlights the total counts from the initial overview page for reports. The tables highlight the details of employees linked to intelligence reports as well as a set of filters for each dataset.

#### **4.6 ControlWorks**

The ControlWorks page highlights the total counts from the initial overview page for ControlWorks. The tables highlight the details of employees linked to incident logs and RoCs as well as a set of filters for each dataset.

## 5 Appendix

### 5.1 Glossary of Terms

<b>WMP / Law Enforcement Terminology</b>	
APP	Authorised Professional Practice
APSP	abuse of position for sexual purpose
BAU	Business as usual
CIS	Continuous Integrity Screening – the ongoing weekly version of the HDW
CoP	College of Policing
CW	ControlWorks
DA	Domestic Abuse
DAL	Data Analytics Lab
FET	Force Executive Team
HDW	Historical Data Wash – national checking of police workforce data against PND
HR	Human Resources
IDVA	Independent Domestic Violence Advisor
ISVA	Independent Sexual Violence Advisor
MARAC	Multi Agency Risk Assessment Conference
NPCC	National Police Chiefs' Council
OPCC	Office of the Police and Crime Commissioner
PCC	Police and Crime Commissioner
PND	Police National Database
POD	People and Organisation Development (Human Resources department)
PPU	Public Protection Unit
PSD	Professional Standards Department
RASSO	Rape and Serious Sexual Offences
RoC	Record of Contact
RV	Recruitment vetting
TRM	Threat Risk Management meeting held daily
VAWG	Violence against Women and Girls
WMP	West Midlands Police