

WEST MERCIA POLICE

MISCONDUCT HEARING:

IN THE MATTER OF PC 3645 JESSICA HINDLEY

BEFORE:

ASSISTANT CHIEF OFFICER: RACHEL HARTLAND LANE

INDEPENDENT PANEL MEMBER: DEVIKA ASSI

INDEPENDENT PANEL MEMBER: MARSHA PEARSON

1. Introduction

1.1 The following paragraphs represent the findings and outcome of the misconduct hearing held at West Mercia Police Headquarters on 25th and 26th February 2026. This misconduct hearing was convened to deal with allegations which the Appropriate Authority (AA) assessed as amounting to gross misconduct. The Officer concerned was PC 3645 Jessica Hindley (hereafter called “PC Hindley” or “the Officer”).

1.2 There may be differences in this written document as compared to any transcript. If that is the case, this written document should be regarded as the definitive version.

1.3 The Chair of the Hearing was Assistant Chief Officer Rachel Hartland Lane. The Independent Panel Members were Devika Assi and Marsha Pearson.

2A. The Pre-Hearing stage

2.1 At the pre-hearing on 10 November 2025 the Chair issued a provisional direction in the following terms: “that as a condition of entry at the misconduct hearing that no person shall write down, record and/or otherwise transmit to or share with any person outside the hearing the following information: anything which would or might reasonably serve to enable the adult arrestee to be identified. This individual is not a witness”.

2.2 The media were invited to make representations on this restriction. No representations were received.

2.3 It was determined, subject to the above, that the hearing be a public hearing.

2B. The Pre-Hearing stage immediately before the hearing commenced

2.4 At the hearing the Chair determined that the direction set out at 2.1 above would apply throughout the proceedings but be kept under continuous review. For the benefit of those members of the press and public attending the hearing the Chair issued further guidance in the following terms so as to avoid jigsaw identification of PC A: “*No person shall record, publish, or communicate any information that would, or might reasonably, lead to the identification of the adult arrestee known as ‘PC A’. This includes any reference to dates, times, locations, police stations, policing divisions, operational units,*

or any contextual detail capable of contributing to jigsaw identification. The individual must be referred to only as 'PC A' in all reporting."

2.5 In the week before the hearing began, the Officer's legal team served the AA with a skeleton argument. This document set out their position that the AA should not proceed with, and the Panel should not determine, a separate but related allegation (Allegation 2).

2.6 The AA accepted the position set out in the skeleton argument and informed the Officer and the Chair that Allegation 2 was to be withdrawn, purporting to rely on Regulation 27 to give effect to this withdrawal. The Panel received legal advice that Regulation 27 concerns the withdrawal of proceedings, not the withdrawal of a particular allegation, and therefore might not be the appropriate mechanism for what the AA intended. As a precaution, the LQP advised the Chair to use her case management powers to invite the AA to seek permission to withdraw Allegation 2 and to make the necessary consequential amendments to the Regulation 30 Notice. Counsel for the Officer raised no objections to the course of action proposed. The Panel decided to: (a) permit the withdrawal of Allegation 2, and (b) allow the consequential amendments to the Regulation 30 Notice. The AA also took the opportunity to make an application that one of the references to a particular time in the Notice be amended. There was no objection and this was done.

2.7 The Chair confirmed a further direction she had made in email correspondence admitting into evidence the following additional material which was served after the Regulation 30 Notice: an additional statement from Sarah Butt exhibiting a "summary search document" (SNB 4) and a further statement from PSI Furniss exhibiting evidence confirming there was no record of faults on West Mercia Police (WMP) IT Service systems Service and an email from [REDACTED] [REDACTED]. The Chair had regard to the written representations made by the respective legal teams as to the exercise of her discretion on admitting further evidence, and noting that there was no objection to the course of action proposed concluded that the material was relevant to the factual issues the Panel had to determine. The Chair considered its admission to be in the interests of justice.

2.8 Finally, in response to an application by the Officer, the Chair exercised her discretion to admit into evidence a bundle containing character references to be considered in the fact-finding stage as this was relevant to credibility and propensity. The AA had no objection to this course of action.

3. Representation and persons involved

3.1 The AA was represented by counsel Mr Holdcroft.

3.2 PC Hindley was represented by counsel Ms Oliver.

3.3 The Investigating Officer was PSI 62777 Andrea Furniss.

3.4 The Hearings Officer was Becky Matthews from PSD.

4. Guidance

4.1 The relevant Home Office Guidance is the February 2020 version.

4.2 The relevant Guidance on Outcomes is the March 2023 version.

4.3 The Code of Ethics was the 2024 version.

5. Material considered

5.1 The Panel were provided with a bundle of 182 pages which included the relevant statutory notices, the edited report from the Investigating Officer and statements from the following witnesses: PSI Furniss, Eirlys Griffith–Reed (Transactions Audit Officer) Sarah Butt (Crime Intelligence Analyst), PS Duncan, Inspector Burrows Jones.

5.2 This bundle also contained an Athena audit, a summary data of computer clicks, search parameters for a custody search, Athena front screen warning declaration and supervisor declaration, an email chain with PSD regarding the Custody Image process, Annual Integrity Health Check [REDACTED] for PC Hindley and relevant screenshots of computer images. In addition, the Panel had the accounts provided by PC Hindley in the 2 interviews conducted with her on [REDACTED]

5.3 The Panel also a copy of the relevant West Mercia Police Data Protection Policy.

5.4 The Panel were provided with the Officer's training record and history.

5.5 The Panel also had the additional material described in paragraph 2.7 above which was contained within a supplementary bundle of 34 pages.

5.6 As set out above the Chair admitted into evidence the character references provided by the Officer.

6. The approach of the Panel

6.1 The approach of the Panel was: (a) To decide on the facts; (b) To decide whether the facts are found proven; (c) To decide whether the Standards of Professional Behaviour are breached and (d) To decide whether any breaches amount to Misconduct or Gross Misconduct or neither.

6.2 The Panel were reminded that:

- The AA bears the burden of proof at all times. The onus is on the AA to prove its case.
- The standard of proof is the civil standard. The Panel's task is not to determine the merely possible, but rather the probable facts i.e. what has more likely than not occurred. The Panel should avoid speculation.

The Panel did not have to resolve each and every issue of dispute between the parties but concentrate on those that are material to the allegations to be decided.

6.3 The Panel reminded itself of the relevant Home Office Guidance: the more serious the allegation or its potential consequences, the more persuasive the evidence must be to satisfy the civil standard of proof. This does not raise the standard itself; rather, the inherent probability or improbability of the alleged conduct is a factor to be considered when determining, on the balance of probabilities, whether the conduct occurred.

6.4 The Panel were advised to bear in mind the wording of the allegations and the response from PC Hindley and, in their review of the facts, to concentrate on what was and what was not in dispute between the parties. PC Hindley did not have to prove anything.

6.5 PC Hindley is of good character. The Panel was advised that character may be considered when assessing allegations of dishonesty. As a general principle, evidence of prior good character can be relevant to both credibility and propensity; someone with no history of misconduct may be viewed as less likely to have acted as alleged, and it may be inherently less probable that a previously blameless individual would engage in serious misconduct for the first time. However, the Panel was reminded not to place undue weight on good character. The High Court has cautioned that such evidence must not overshadow the primary focus on the evidence directly relating to the alleged wrongdoing.

7A. The Regulation 30 Notice

7.1 At the material time PC Hindley was working as a constable seconded to the Criminal Justice Youth Offending Team (paragraph 1 of the Notice).

7.2 On the day in question PC Hindley was on a rest day. At 19:52:06 (BST) she conducted a search on the Athena computer system for arrests between that day and the preceding 2-day period for custody one of the police divisions of WMP (paragraph 2).

7.3 The search produced 27 custody records. None of the records related to youths that had been arrested during the period searched (paragraph 3).

7.4. Within the 27 custody records results was the custody record for PC A who had been arrested on a date within the search parameter period (paragraph 4).

7.5 At the time of the search PC A was known to PC Hindley as a colleague (paragraph 5).

7.6 At 19:52:28 (BST) on the day on question PC Hindley clicked on the custody record of PC A (paragraph 6).

7.7 At 19:52:28 (BST) on the day in question PC Hindley accessed the custody record for PC A and accessed the data held within that custody record (paragraph 7).

7.8 PC Hindley had no legitimate policing purpose to access the custody record of PC A (paragraph 8).

8. The Opening – How the AA put the case

8.1 Mr Holdcroft set the scene by outlining the regime in respect of how the police and police officers should manage information and data. He said that the management of police information is governed by a Statutory Code of Practice and the Approved Professional Practice (APP) on Information Management. These set out that police information may only be shared when it is linked to a legitimate policing purpose. Such purposes include:

- Protecting life and property.
- Preserving order.
- Preventing and detecting offences.
- Bringing offenders to justice.
- Fulfilling any duty arising from common law or statute.

8.2 Mr Holdcroft further said that Officers must only access information when they have a lawful and legitimate reason to do so. They are regularly reminded of their responsibilities around data protection and confidentiality, including through mandatory training and system login notices.

8.3 Mr Holdcroft pointed out that the Officer had received training in relation to data protection and confidentiality.

8.4 Mr Holdcroft brought to the attention of the Panel relevant extracts from the WMP Data Protection Policy and emphasised the following passages (emphasis added):

*“It should be stressed that curiosity is **not** a valid reason for carrying out checks on police information systems. Listed below are some examples of obtaining personal information that are not covered by our registered purposes it should be noted that the list is in no way exhaustive: Using both national/local information systems to check **out conviction status** of acquaintances including family, friends’ neighbours etcUsing the force intranet system to **check work colleagues’** personal details i.e. home address, marital status, date of birth viewing of photographs etc.... Examples of data breach are provided below:deliberate or accidental action or inaction by a controller or processor.... Where a personal data breach has occurred a security information form must be completed without delay.”*

8.5 The Policy also references Section 170 of the Data Protection Policy (DPA) which makes it a criminal offence to recklessly obtain, disclose or retain personal data without the consent of the data controller.

8.6 Mr Holdcroft went on to set out what he said happened on the day of the Athena search when the Officer allegedly accessed the custody record of PC A without a policing purpose. Details of what occurred are set out in the analysis of the evidence of Sarah Butt and the findings section of this document.

8.7 Mr Holdcroft pointed out that before accessing the Athena system officers are required to confirm that they will only use the system for a legitimate policing purpose. They are further warned that if they misuse the system, they may be liable to prosecution, disciplinary action or both. They must confirm that they accept the conditions before accessing the system.

8.8 As part of his case Mr Holdcroft referenced the fact that on [REDACTED] an Athena Audit Request was sent to the Officer in relation to the access. Details of this request and the response are set out in the findings section of this document. There was a delay in the response and the Officer had to be sent reminders. In order to answer the request, the Officer had to access the custody record before submitting her return. On [REDACTED] [REDACTED] the Officer completed her Annual Integrity Health Check (AIHC) in which she stated that she had not used police systems for a non-policing purpose since her last AIHC.

8.9 Mr Holdcroft said that on [REDACTED] [REDACTED] was arrested and taken to a West Mercia Police Station where their photograph was taken and recorded on a custody record / detention log. He said that the evidence showed that PC A's photograph would have been visible to any person who accessed this custody record.

8.10 In his opening Mr Holdcroft emphasised the length of time that record was open and displayed on the screen which was 1 minute and 40 seconds (100 seconds). He also said that once open PC A's picture would have been instantly visible to the Officer and it was inexplicable that she did not close it down sooner. He argued that it was no coincidence, and could not be explained away as an accident, that out of the 130 or so detained persons whose records were presented to the Officer on [REDACTED] she clicked on a line opening up the record of a serving police officer whom she had met before. Mr Holdcroft pointed out that this was an adult record and the Officer was searching for youths (the legitimate policing purpose) and it was obvious who was an adult or a youth when using the system since dates of birth were presented as part of the information displayed before the user clicked on an entry.

9. The position of the AA regarding the Standards of Professional Behaviour (SPB)

9.1 The amended Regulation 30 Notice set out that it was alleged that PC Hindley was:

In breach of the Standard of Honesty & Integrity in that she accessed data relating to PC A when she knew, or ought to have known, that she had no proper policing purpose to do so.

In breach of the Standard of Confidentiality in that she:

- a. accessed data relating to PC A without a proper policing purpose.
- b. accessed data relating to PC A without a proper policing purpose in breach of the West Mercia Police Data Protection Policy.

In breach of the Standard of Orders and Instructions in that she accessed data relating to PC A without a proper policing purpose in breach of the West Mercia Police Data Protection Policy.

In breach of the Standard of Discreditable Conduct in that she acted in a way that discredited the Police Force in that she acted dishonestly and accessed confidential data without a proper policing purpose.

9.2 In his submissions Mr Holcroft indicated that the AA did not rely on the honesty limb of the Honesty and Integrity Standards and the Panel should consider Integrity only.

10. The evidence of Sarah Butt

10.1 Sarah Butt was the only witness who gave oral evidence to the Panel during the presentation of the case for the AA.

10.2 Sarah Butt was employed by WMP as a Crime Intelligence Analyst. As part of her role, she had access to the audit functionality in Athena, which allowed her to perform a search for what Athena¹ entities employees had looked at within a given time period. She reviewed an Athena audit of which employees had looked at the custody record for PC A who was arrested on [REDACTED]

10.3 Sarah Butt could replicate what had happened on the Athena system at the relevant time by way of a reconstruction and generating screenshots – one of these screenshots was the custody access dashboard details of PC A which the audit showed what the Officer had accessed. These details included a photograph of PC A – [REDACTED] full name, date of birth, address, gender, ethnicity and occupation (shown as “Police Service”).

10.4 Sarah Butt produced four exhibits in her evidence. The first exhibit was SNB/01 - which showed transaction lines from the Athena audit. SNB/02 summarised the Officer navigating the Athena record. The next exhibit was SNB/03 a reconstruction of the

¹ Athena is a web-based Records Management System and intelligence platform used to manage investigations, custody and case preparation.

search parameter results for [REDACTED] Division for the relevant period which brought up 27 custody records.

10.5 The final exhibit was SNB/04, a more detailed summary of SNB/01 introduced as additional evidence containing details of actions namely: the number of custody records brought up in each divisional search and whether they belonged to an adult or youth and any particular custody record then opened – it then recorded the time duration between any such action and the previous action. Saran Butt was taken through SNB/04 by Ms Oliver not by way of challenge but to seek clarifications and explanations.

10.6 The Panel considered that the main takeaways from this evidence were as follows:

- The audit showed that the Officer searched each Division individually in the order: [REDACTED]
- There were minor issues such as what appeared to be the automatic reopening of a record or a one second time delay in loading an image – these appeared to be of no consequence.
- The integrity of SNB/04 as an exhibit that could be relied on was not challenged and likewise the technical evidence provided by the Athena audit could be relied on.
- The Officer opened a custody record relating to an adult in the [REDACTED] Division search - this was open for 21 seconds.
- The search results for [REDACTED] division records 21 records with no youths and none of the records are clicked on – there are then 50 seconds until the next search is conducted.
- The custody dashboard details for PC A in the [REDACTED] Division search remained open for 1 minute 39 /40 seconds.
- The screenshot reconstruction which illustrated the work that Sarah Butt had done on the audit based on exhibits SNB/01-03 was not challenged either at the hearing or by the Officer when she was interviewed by the investigating team.

11. The Case for PC Hindley – the Regulation 31 Response (part 1)

11.1 The Officer set out her response to the allegations as follows:

“1. The Officer does not remember clicking on the custody record of PC A on [REDACTED] [REDACTED] If she did access the record, this was accidental. The Officer does not accept that accidentally accessing a custody record amount[s] to Misconduct or Gross Misconduct

2. The Officer gave an honest account of her actions in the audit request she completed on [REDACTED]

Detailed response to Allegations Knowledge of PC A

3. The Officer believes that she has met PC A on two or three occasions at the most. The only specific memory she has of meeting PC A is when [REDACTED] was introduced to her by her colleague [REDACTED] Police station. This was several years before the relevant events. [REDACTED] was introduced to her as [REDACTED] The Officer did not know [REDACTED] last name, [REDACTED]

4. The Officer was unaware that PC A was working from the same police station as her between [REDACTED] There are roughly [REDACTED] people working at [REDACTED] police station. The building is spread over [REDACTED] floors. [REDACTED]

[REDACTED] The Officer never had any reason to enter the [REDACTED] office during her time at [REDACTED] There are many officers working from the station who the Officer would not recognise.

Actions on [REDACTED]

5. In [REDACTED] the Officer was seconded to the Youth Justice Service covering the [REDACTED] area. Her role was to act as the link between the Youth Justice Service and West Mercia Police.

6. One aspect of the job was checking Athena multiple times a day to see whether any youths had been arrested. The team have a daily remand officer who attends court, and the Officer's job was to ensure that this officer had all of the information needed for the court hearing. The Officer would therefore search Athena to see if any youths had been arrested, and if they had, she would obtain the relevant information from their custody record and send it to the remand officer.

7. When the Officer started the role, she would carry out this task on the morning of the court hearing. However, she quickly realised that this was a very difficult task to complete on a Monday morning because several youths may have been arrested between Friday and Monday. She therefore decided that it was much more effective to conduct the search between 18:00 and 20:00 on a Sunday evening. This ensured that the remand officer always had the necessary information for the court hearing the next day. This approach was approved by her Sergeant.

8. The Officer's usual process when completing these searches is as follows.: She inputs the relevant arrest date and the custody facility ID. She does not use the 'date of birth from' and 'date of birth to' function because she is also searching for any relevant information about the parents of the youths who are in the system. She clicks 'search' and then scrolls through all of the results that appear. The Officer will look at both the 'name' column and the 'date of birth' column when analysing the results, because again, she is also looking for any relevant information about associated adults. Some youths and their families come to the attention of the police repeatedly, and so the Officer will often recognise certain names when completing her checks.

9. On [REDACTED] the Officer was completing her usual Sunday evening checks. She accepts that she would have searched for arrests between [REDACTED] and [REDACTED]

██████████ on █████ Division ██████████ although she has no specific memory of doing so. The Officer has no memory of clicking on the custody record for PC A. She does not remember seeing █████ picture. She did not realise that she had accessed the record of a serving police officer.”

12. The Case for PC Hindley – the Regulation 31 Response (part 2)

12.1 The case against PC Hindley referenced her actions following on from the events of ██████████ The Officer responded to this aspect of the matter as follows:

Response to the audit request

“10. The Officer accepts that she was sent an Athena audit request on ██████████ asking her to explain why she accessed the custody record for PC A.

11. There was a delay in replying to the request. As per the email sent by the Officer to Sergeant Duncan on ██████████ she had a considerable workload at the time and therefore she believes that she simply forgot to complete it. She was also on leave between ██████████

12. In order to work out which record the audit request related to, the Officer used the transaction detail number to complete the search again. She saw the custody record of PC A. There was a photo on the record, and the Officer recognised the picture. She realised that the record did not relate to a youth or an associated adult. The Officer was completely transparent about that fact in the audit response, where she stated that the person did not relate to her youth work, and she inferred that the record was accessed by mistake. She did not try to cover up her mistake, and her response was entirely honest.

13. The Officer sent the audit response to her line manager, Sergeant Duncan, who did not raise any issues with her account. She did not know what an SR1 form was, or when it should be used. She believed that she had responded appropriately by filling in the audit request”.

13. The interview response from PC Hindley

13.1 In her interviews with the investigating team on ██████████ the Officer said that:

- She had about 22 years’ service.
- She understood the rules for using police systems.
- She would be looking for people with a date of birth of 2006 or above.
- She did not recollect clicking on PC A’s record.
- She did know PC A and she had met PC A before – the person was introduced to her as ██████████
- She should not have been viewing PC A’s record.

- The photograph of PC A did not “register” with her at the time and she had no memory of it being on the screen at the time.
- The period of access (around 1 minute 40 seconds) was a long time.
- She did recognize PC A from the photograph when she later went onto the system to complete the requested audit.
- It was an accidental “click” and with an accidental click, submitting an SR 1 form would have been the right thing to do to report it.

14. The evidence of PC Hindley

14.1 The Officer began by outlining her background, noting that she joined WMP in July 1983. She described meeting PC A only once between [REDACTED] - a brief introduction [REDACTED]. She said she never learned their surname, had no further contact and, although [REDACTED], they worked [REDACTED] [REDACTED] had no overlapping duties, and no social interaction.

14.2 The Officer explained that data protection was embedded in her daily work, though she knew human error was common, especially as she shared a name with another officer, leading to misdirected emails. She outlined her Youth Justice Officer role, including weekend duties.

14.3 The Officer said she had no clear memory of [REDACTED] and accepted she was reconstructing events in her mind when giving her version of events. She suggested domestic distractions whilst working from home might have played a part in any mistake she made, though she had own office to work in. She acknowledged that an earlier explanation she had proffered —that she clicked PC A’s name because it appeared between two youths—was speculative and incorrect.

14.4 The Officer described her usual custody-check workflow: opening Athena, copying required information, pasting it into an email, and switching back. She said she searched the [REDACTED] window for offender-management purposes, scanning for juveniles and sometimes opening linked adult records. She noted the audit showed one youth record opened twice, which she could not explain, and said the timings were consistent with her normal process.

14.5 Addressing the suggestion she had “just happened” to click on PC A’s record among 130 results, the Officer pointed out she had also opened another adult record. She accepted she was on PC A’s record for 1 minute 40 seconds and recognised the seriousness of this, but maintained it was an unintentional mistake. She said she would have reported it immediately had she realised at the time.

14.6 The Officer said that she was so used to performing the tasks on the system that she could not recall whether she had to double click on the record or whether a single click would suffice. She added that when working from home she was using one screen, she did not use a mouse and used the touch pad instead.

14.7 The Officer explained that opening the other adult record for 21 seconds could have been legitimate, as she often checked adults linked to youths. She also noted Athena could load slowly on her home Wi-Fi.

14.8 Mr Holdcroft challenged the Officer about her claim that she did not see PC A's photograph and the detail on the custody record dashboard pointing out that this conflicted with the technical evidence and was an attempt to avoid admitting misconduct. In response the Officer maintained that she had not seen the photograph/record.

14.9 The Officer explained she received the audit request on [REDACTED] went on leave shortly after, returned on [REDACTED] to a backlog and apologised on [REDACTED] for the delay. She said she only understood the reason for the audit query when she reviewed the audit trail on [REDACTED] and accepted that she had accessed the record in error.

15. The Character Evidence

15.1 As part of the case for the Officer the Panel considered the character references, these references are examined and discussed later in this document.

16. Closing Submission from Mr Holdcroft

16.1 Mr Holdcroft argued that the Officer's account was not credible. Out of roughly 130 detainees, she accessed PC A's record and the chance of doing so accidentally was minimal. He said there was no evidence of delay or system mis-loading and that her explanation required an implausible sequence of steps namely reviewing records, adjusting searches and navigating screens before "accidentally" selecting PC A. He submitted this was incompatible with inadvertence.

16.2 Mr Holdcroft further argued that the account from the Officer required two unlikely errors: clicking the record and then failing to notice the photograph. If the first was accidental, the second could not be. Screenshots also showed that she accessed the record more than once, contradicting her claim otherwise. The record was open for 100 seconds, during which she must have seen the photograph. He concluded the only reasonable inference was that she was not doing what she claimed, and that her later explanation was constructed to avoid admitting misconduct.

17. Closing submission from Ms Oliver

17.1 Ms Oliver accepted on behalf of the Officer that the record was open but said the issue was whether the Officer intentionally viewed it. She argued the audit cannot show purpose or observation—only that the record was accessible for about 100 seconds. She said the Officer did not know PC A's surname until [REDACTED] and would not have recognised the name or pronunciation, undermining any suggestion of deliberate selection.

17.2 Ms Oliver submitted that an accidental click is human error, not misconduct, which requires culpability. There was no evidence of intentional access, no basis to think the Officer recognised the record and no personal or professional link that would give motive. She argued that the most plausible explanation was an inadvertent click while switching between Athena and email under time pressure. Ms Oliver added that the audit showed no scrolling or further interaction and no evidence that she viewed any data.

17.3 Ms Oliver said that the 100-second interval was consistent with routine tasks, including recording negative searches and with normal household distractions on a Sunday evening. She further said that the Officer had consistently said she did not recall seeing the record and had only tried to reconstruct events and that her mistaken assumption about youth entries was an honest attempt to understand the error before learning that none appeared in that search.

17.4 Ms Oliver argued the Officer's audit response was routine and delayed only by leave and workload and there was no reason she should have mentioned the record related to a colleague. Finally, she said that the Officer's long, unblemished service supported her credibility and made it unlikely she would risk her career out of curiosity, especially knowing the system was auditable. She concluded that the evidence supports accidental, unnoticed access, falling short of misconduct, let alone gross misconduct.

18. Findings of the Panel

Introduction to the task of the Panel

18.1 The Panel reviewed the evidence in this case. It sought to ascertain the facts (whether admitted or proved).

18.2 The Panel examined the Regulation 30 Notice and the admissions made in the Regulation 31 Response. It considered the technical evidence of the Athena audit, which was not challenged, and the evidence of the Officer. Mr Holdcroft put the particulars of the allegation to the Officer who did not dispute the individual particulars as such but said that, so far as paragraph 5 of the allegation was concerned, she did not know the details of PC A's full name. The Officer also added a rider to her admission in respect of paragraph 7 that she accessed the custody record for PC A by saying that, although the evidence showed that she accessed the custody record, she did not see any data.

18.3 The AA made the helpful concession that the Officer knew PC A by a different given name (she knew the person as [REDACTED] and did not know their surname until [REDACTED]). The AA also accepted that the pronunciation of the name as it appeared on the Athena system would not have alerted the Officer to PC A's identity.

18.4 This leaves the only factual issue between the AA and the Officer that needs to be determined is whether PC Hindley “accessed” the data within the custody record.

18.5. Mr Holdcroft had said matters contained within the allegation are not matters of strict liability, nor is it a case where the majority of the facts in the allegation are in dispute. The issue from the AA’s point of view was whether the Officer knew what she was doing or not.

18.6 On behalf of the Officer Ms Oliver had said it was accepted that the custody record for PC A was opened and visible. She said that the issue for the Panel is not whether the record appeared on the Officer’s screen, but the circumstances in which it was opened and whether it was actually viewed.

What happened on [REDACTED]

18.7. On [REDACTED] PC A (the detainee) was arrested and taken into custody. At approximately [REDACTED] the detainee’s photograph was taken and recorded on a custody detention log, making it visible to anyone who accessed [REDACTED] custody record.

18.8. On [REDACTED] (a Sunday) the Officer was working from home. As a Youth Justice Officer, she was required to access custody records to identify which young people had been arrested and whether any were likely to be remanded. If a young person was remanded, the Youth Justice Service needed to be notified immediately so that a remand officer could attend court. The role therefore required regular checks - several times a day, not just once in the morning - to ensure they were aware of any youths in custody and could prepare the necessary support.

18.9. The Monday checks were demanding because they covered arrests from Friday evening to Sunday night, often requiring the Officer to review a high volume of cases and prepare remand documents for any youths held over the weekend. To manage this, the Officer routinely carried out the checks on Sunday evenings - anywhere from 20 minutes to two hours depending on arrests - usually between 6 and 8 p.m., ensuring everything was ready for the remand officer. This was her usual practice and had been approved by her line management. On Monday mornings she would log in around 6:30 - 6:45 a.m. to see if any new arrests had come in overnight; if not, she could simply send the email prepared the night before, avoiding the pressure of trying to complete hours of work first thing in the morning while racing to meet court deadlines.

18.10. It was not disputed that to complete her work properly the Officer had to conduct searches across all 5 Police Divisions in West Mercia. It was also not in dispute that, having regard to her wide Youth Justice remit, the Officer would on occasion legitimately search the records of adults arrested as they could be co accused, parents or be otherwise associated with known youth offenders (which the Officer would need to know about given her remit relating to interventions and diversions).

18.11. At 19:41, the Officer conducted a search within [REDACTED] Division. She accessed 40 custody records - 38 adults and two youths. She viewed the first youth's record for a total of four minutes and four seconds (1:51 and 2:13). She viewed the second youth's record for five minutes and twenty seconds (1:21 and 3:59).

18.12. At 19:50, the officer carried out a similar search [REDACTED] Division, reviewing 21 adult custody records. She viewed one record belonging to an adult detainee with a date of birth in May 2005 for 21 seconds.

18.13. At 19:51 The officer then repeated the exercise in [REDACTED] division examining 21 custody records, all relating to adults. She did not access any of these records.

18.14. At 19:52:06, she conducted the same exercise for [REDACTED] division. There were 27 records, each showing a surname, given name, date of birth, and gender of the detainee. None of the records related to youths. Within the 27 custody records was the custody record for PC A.

18.15. The Officer accepts that at 19:52:28 she clicked on the custody record for PC A and does not challenge the Athena audit on this point – she says that she must have clicked in the row of the screen containing the names of arrestees which contained the name [REDACTED] by accident. Further the Officer agreed that once the name had been clicked a “View Record” Dashboard is automatically opened.

18.16 The Officer then conducted her final search on [REDACTED] Division examining one youth custody record – the time taken was 11 seconds.

The evidence of Sarah Butt

18.17. The evidence of Sarah Butt is summarised in paragraphs 10.1 to 10.6 above and is supported by her exhibits and the screenshots. It was noted that Sarah Butt had carried out a reconstruction. As a result, we cannot know from these exhibits:

- the exact order in which the custody records appeared to the officer, or
- which records appeared immediately above or below the PC A record.

18.18 Sarah Butt also said that the Athena audit does not capture scrolling behaviour. Therefore, if the Officer scrolled up or down within the record, that would not appear in the audit. She described the audit as “neutral” as to whether any such interaction occurred. It was agreed and not a matter of dispute that the audit also could not show:

- whether the Officer had emails open.
- whether any internet tabs or documents (e.g., Word) were open.
- whether the Officer was interacting with any other application.
- or whether the Officer was actually looking at the custody record for PC A at the time.

After [REDACTED]

18.19 The Police Systems Transactions Officer sent the Officer an Athena audit request on [REDACTED] regarding her access to records at 18:52 on [REDACTED]. After receiving no reply, she issued a reminder to PS Kerr Duncan on [REDACTED]. With still no response by [REDACTED] she escalated the matter to second line manager, Claire Munn. Later that same day she received a reply from PS Duncan, who returned the required countersigned audit declaration, although it was unsigned.

18.20 In response to the question *'For what policing purpose was the transaction made?'* PC Hindley provided the following response: *"I am a seconded YJS officer. Part of my role is to check the custody blocks daily for any new youth related arrests. I conduct my weekend checks from my laptop on a Sunday evening for the weekend that has just been, this is to enable me to forward any relevant details to the remand officer for the following morning who is required to attend court. I believe I must have selected this record in error at the time as the person is not a youth – but can only surmise they may have been next to a youth in the list of arrests"*. The response in relation to PC Hindley's working hours that day was: *"RD – however as explained above I conduct the custody checks for the weekend on a Sunday evening to be able to forward any relevant details to the remand officer for the following morning who is required to attend court."* The response in relation to any data being passed to any other person was: *"No"*.

Analysis

18.21 The Panel considered the evidence indicating that the Officer had deliberately accessed the custody record. This included the length of time the record remained open, which was accepted to be approximately 100 seconds. The Panel also noted what was said by the AA to be the improbability of it being a coincidence that the record opened related to a serving police officer, and that such access occurred through an accidental click.

18.22 The Panel further considered the Officer's account. She stated that she had no recollection of viewing the dashboard/record, including the photograph of PC A contained within it. She maintained this position consistently throughout her interviews with the investigating officers and again when giving evidence before the Panel. However, the Panel further noted this account to be inconsistent with the known technical evidence, which showed the record was open for a significant number of seconds. A reasonable inference to draw was that the Officer must have seen the contents at some point with the photograph prominently displayed as the most significant feature within it.

18.23 The Panel reminded itself that the Officer was engaged in this activity on a Sunday evening for a period of 20 minutes or so. In the context of her task - checking 5 divisions - this was a relatively short period of work. It therefore appeared that a not insignificant portion of that time was spent dealing with this particular record. The audit

further showed that the Officer had opened another adult record, but for a significantly lesser time period.

18.24 The Panel considered the evidence advanced in support of the contention that the initial click which opened the custody record had been accidental. The Panel accepted the evidence that the Officer did not recognise the name of PC A when it first appeared to her on the Athena audit as one of 27 arrestees within [REDACTED] Division.

18.25 The Panel further noted that there was no evidence that the Officer had disseminated the information, acted upon it, or shown any particular interest in it. Her previous association with PC A had been brief and had occurred approximately two years before the incident. There was nothing to suggest any ongoing connection or motive.

18.26 The Panel took into account the limitations of the audit evidence, as previously outlined, including what the audit could and could not reliably demonstrate.

18.27 In reviewing the audit evidence, the Panel recognised that not all of the approximately 100 seconds during which the record was open would have been spent examining its contents. The Officer was required to send a nil return in relation to youth arrestees, and this task would have occupied part of that time. Ms Oliver said that this could have accounted for as much as 50 seconds, based on previous activity on Athena. The Panel noted that the AA said that having regard to what was required - namely, to input or copy and paste a nil return that 50 seconds was likely too generous an estimate to complete such a task. Balancing these competing arguments and being generous to the Officer and subtracting 50 seconds – this still left an equivalent length of time unaccounted for (i.e. almost a minute).

18.28 The Panel considered the Officer's explanations regarding the circumstances in which she completed her task on the Sunday evening in question. She had an office at home from which she worked and the task occupied her for around 20 minutes. Her recollection of those events was vague and speculative save for her consistent assertion that she did not see the photograph contained presented in the record. She maintained this position throughout the investigation and again before the Panel.

18.29 The Panel did not place significant weight on the Officer's references to possible domestic distractions. It accepted that she was simply trying to reconstruct why she believed she had not seen the photograph. The same applied to her response to the audit review, where she answered the questions posed and speculated - incorrectly, as it later emerged - that she had clicked on PC A's name because it appeared between two youth entries.

18.30 The Panel noted that the Officer said that she only realised the audit concerned a potential breach involving a serving officer's record when she legitimately accessed the file to complete the audit questionnaire. The Panel have their doubts about this explanation bearing in mind the length of time the record was open even if the first click

was accidental. It noted that she did not appear to pause and consider why the request was being made of her in the first place or seek line management advice. The Panel considered that she could have been more forthcoming in her response and may have been guarded because she understood a breach had occurred.

18.31 The Panel noted her good character and took this into account positively in terms of an assessment of her credibility and her propensity to have deliberately set out to commit a data breach. This evidence was weighed in the balance and given appropriate weight.

Conclusions

18.32 The Panel were of the view that given the strength and nature of the evidence as set out and analysed above that, on balance, it could not find that the Officer deliberately and in a targeted way made the initial click on the record recognising PC A's name and at that point accessing the record for reasons of curiosity. The inferences drawn from the available evidence were not strong enough to support such a finding on the balance of probabilities. The mere improbability of accidentally clicking on a serving officer's file was not, in itself, enough to establish that the Officer's actions were deliberate from the outset.

18.33 Notwithstanding the above finding the Panel noted that the record was open for 100 seconds. The Panel was satisfied that the custody access dashboard details as shown in the screenshot, was open for this period of time and that when the Officer moved from any other open tab back to this record, she would have seen the image of the custody photograph and the occupation of the detainee, namely that he was a police officer – this in itself is sensitive data. The Panel had noted the Officer was working off one screen only and her only other task was to draft an email.

18.34 The Panel were of the view that, on the basis of the audit records, tasks such as drafting a standard draft email for a nil return as it was for [REDACTED] Division would not have taken too much time out of the 100 seconds. The context was that this was the penultimate search the Officer undertook that day – she had one more Division to search and was only on the system for a few more seconds. The total time taken on the searches of all 5 Divisions and conducting any associated tasks was around 20 minutes.

18.35 There is no evidence before the Panel of the Officer scrolling through the record or actively searching for further entries. However, the photograph and occupation of PC A would have been immediately visible on the custody access dashboard. On that basis, the Panel concludes that the Officer accessed data within the record without any legitimate policing purpose. She did not close the record promptly; while a short period of grace would have been reasonable, the length of time the record remained open and accessed went well beyond this. This constituted a data breach and should have been reported and recorded accordingly.

18.36 The Panel rejects the Officer's account that she had not seen the photograph and/or the data showing the detainee was a police officer. This was inconsistent with the evidence and the analysis set out above. The Panel is reluctant to speculate on why the Officer adopted this position in interview and in her evidence, but she appeared to have convinced herself that she had not seen the photograph and maintained that position throughout. The Panel also noted that some of her assertions were speculative, and she appeared prone to reconstructing events based on what she believed had occurred rather than on what the evidence demonstrated.

18.37 The Panel has not found that the Officer deliberately targeted PC A's data. However, it notes that the Officer accepted, during the audit response, that she recognised PC A from the image and that the photograph was a likeness of how PC A appeared.

18.38 The Panel is not required to determine a motive for the conduct, but observes that it is human nature to be curious about information of this kind, and it is not unreasonable to consider that curiosity may have been a factor in this case.

18.39 Accordingly, the Panel find the facts as set out in paragraphs 1 to 7 of the Regulation 30 Notice proved (accepting that the Officer did not know PC A's full name). Having regard to all the above and the analysis of the evidence, the Panel make a finding of fact that the Officer accessed the custody record for PC A and accessed the data held within that custody record albeit on the basis set out in the preceding paragraphs.

19.The Standards of Professional Behaviour

19.1 The Panel, having made the factual findings set out above, proceeded to consider whether the Standards of Professional Behaviour were engaged and breached. The Panel first considered the Standard of Confidentiality. The facts proved demonstrated that the Officer accessed data relating to the PC A without a proper policing purpose, in breach of the West Mercia Police Data Protection Policy. The Panel was satisfied that this amounted to accessing police information without lawful justification.

19.2 The Panel further determined that the standard of Orders and Instructions was engaged. By accessing data relating to PC A without a proper policing purpose, the Officer acted contrary to the clear requirements of the West Mercia Police Data Protection Policy. The conduct under scrutiny concerned the Officer's failure to handle confidential information and police data in accordance with the guidance and instructions she was required to follow. She is an experienced officer, accustomed to handling sensitive information, and was entrusted to do so appropriately. She had also recently completed her Data Protection training [REDACTED]

19.3 During the course of proceedings, the allegation that the Officer had acted dishonestly fell away. This left the question of whether the standard of Integrity - in the sense of doing the right thing - had been breached. The Panel concluded that the

conduct was most accurately categorised as a breach of Confidentiality and of Orders and Instructions. The Panel was not persuaded to make a positive finding that the Standard of Integrity had been breached, nor that Discreditable Conduct was engaged, as the latter had been pleaded specifically in the context of alleged dishonesty.

19.4 Having regard to the threefold purpose of police misconduct proceedings - maintaining public confidence, upholding high standards, and protecting the public - the Panel recognised the importance of confidence in the handling of police data and the potential consequences of data breaches. In that context, the Panel found that the Standards of Confidentiality and Orders and Instructions were not only engaged but had been breached.

20. Gross Misconduct or Misconduct

20.1 The Panel considered the tests for Gross Misconduct and Misconduct.

20.2 Under the 2020 Regulations, “misconduct” means a breach of the Standards of Professional Behaviour so serious as to justify disciplinary action and “gross misconduct” means a breach of the Standards of Professional Behaviour that is so serious as to justify dismissal.

20.3 The Panel considered it useful at this stage to consider the College of Policing Guidance (“the Guidance”) on outcomes to make a preliminary assessment of culpability and harm to assist it in assessing where this conduct landed on the spectrum of seriousness.

20.4 The relevant extracts from the Guidance are as follows:

[Paragraph 4.34]: *“The misuse of police computer systems or confidential police information more generally is a particular concern for the police service. Police computer and manual systems hold a significant amount of information about members of the public. Most of this is sensitive, and it is both a public expectation and a legal requirement that information obtained during the course of policing duties should be treated in strictest confidence, properly protected and used only for legitimate policing purposes”.*

[4.35] *“Under no circumstances should anyone access or use police information for personal benefit. Personal reasons for accessing confidential police information, such as general curiosity or a desire to check on criminal activity near an officer’s home, are not acceptable. If an officer is accessing police information not available to the general public, there should always be a specific and proper policing purpose for doing so”.*

[4.36] *“Accessing confidential police information without a legitimate policing purpose is an abuse of an officer’s position and may merit dismissal in serious cases. Accidental access to information without a legitimate policing purpose will not attract such an outcome”.*

[4.37] “Factors *that support a more serious outcome include:*

- *accessing information of a secret nature or high classification*
- *onward disclosure of the information*
- *malicious motive for accessing or disclosing the information*
- *personal gain*
- *actual or potential compromise to a police investigation*
- *breaches of personal privacy where the data is very sensitive*
- *attempts to cover up improper accessing of data*
- *altering information held by the police”*

20.5 The findings of fact do show that the Officer was culpable and this was not a technical breach of confidentiality, although it lacked the aggravating feature of being targeted. The fact of a police officer being arrested is in itself sensitive and could be argued to be very sensitive and such information does require careful handling and protection. That being said the conduct did not contain any of the more egregious features set out in the bullet points above, in particular there did not appear to be any malicious motive.

20.6 The Officer accessed confidential information without a proper policing purpose, contrary to policy, and in circumstances where she was expected to exercise care and professionalism in handling particularly sensitive data relating to the arrest of a police officer whom she knew.

20.7 After careful review the Panel came to the view that the conduct fell just short of being categorised as gross misconduct. The allegations as opened by the Appropriate Authority were not proved in several significant respects - namely, no dishonesty, no lack of integrity, and no deliberate targeting of the PC A but the Panel nevertheless concluded that the proven conduct comfortably crossed the threshold for misconduct but was not gross misconduct. This was a finely balanced decision and reflected the particular circumstances of this case and the basis on which the allegation was found proven including context and most importantly how long the record was open for (100 seconds).

20.8 Accordingly, the Panel found that the Officer’s conduct amounted to **misconduct**.

21. Outcome

The representations from Mr [REDACTED] from the AA

21.1 Mr [REDACTED] argued that the conduct was deliberate, the risk of harm was clearly foreseeable. He said it involved accessing highly sensitive personal data for personal reasons, which the Data Protection Act 2018 explicitly prohibits. He said such breaches require the affected person to be informed, causing understandable distress and anxiety, particularly when the misuse comes from within the organisation.

21.2 Mr Holdcroft said that the Officer's actions undermined public confidence, especially given the expectation that police officers protect sensitive information and uphold the law. Her behaviour was intentional, driven by curiosity, and continued over a period of time. She ignored supervision, failed to follow procedures, and provided incomplete audit responses. The victim was vulnerable due to their arrest, increasing the seriousness of the misconduct.

21.3 The AA argued that a final written warning for five years was appropriate. Mr [REDACTED] asserted that while the Officer's character was considered, personal mitigation was limited because her actions directly threatened public trust and confidence.

The representations from Ms Oliver for the Officer

21.4 Ms Oliver pointed out that the Panel had made no findings of dishonesty, no breach of integrity, no discreditable conduct, no deliberate targeting of PC A, and accepted that the initial access was accidental.

21.5 Ms Oliver said that this incident must be viewed as a clear anomaly in an otherwise exemplary 23-year career marked by dedication and integrity. That history is a significant mitigating factor and should not be given little or no weight.

21.6 Ms Oliver said that a written warning was the proportionate outcome when the circumstances are properly considered. She argued that the key points supporting this were:

- The conduct was not planned, targeted, or premeditated; it falls far below the threshold for high culpability.
- Public confidence must be assessed from the perspective of an informed member of the public, who would understand the accidental nature of the initial click, the extremely brief access (under 100 seconds), and the absence of any sharing or misuse of information.
- No evidence of harm to PC A has been presented.
- This was a single, momentary lapse of the briefest duration.
- The officer was engaged in legitimate policing activity before and immediately after the incident, reinforcing that this was an isolated mistake within otherwise proper work.
- The misconduct arose from a single click, reflecting minimal involvement.

21.7 In terms of its approach to outcome the Panel was reminded of and reviewed the latest version of the Guidance. The Panel considered the three-stage, structured approach referenced in *Fuglers LLP v SRA* [2014] EWHC 179 (Admin).

21.8 The three-stage process set out in the Guidance on page 15, is as follows: Stage 1: assess the seriousness of the misconduct by reference to: (i) the officer's culpability

for the misconduct; (ii) the harm caused by the misconduct; (iii) the existence of any aggravating factors; (iv) the existence of any mitigating factors. Stage 2: keep in mind the purpose of imposing disciplinary action. Stage 3: choose the disciplinary action which most appropriately fulfils that purpose for the seriousness of the conduct in question.

21.9 The Panel kept in mind at all stages the three-fold purpose of imposing disciplinary action in police misconduct proceedings.

Stage 1: Seriousness

21.10 Stage 1 requires an assessment of the seriousness of the Officer's conduct which was found proven taking into account culpability, harm, aggravating and mitigating factors. The Guidance explains **[paragraph 4.1]** that *"assessing the seriousness of conduct lies at the heart of the decision on outcome..."*

Culpability

21.11 The Guidance sets out the following:

[4.9] *"Culpability denotes the officer's blameworthiness or responsibility for their actions. The more culpable or blameworthy the behaviour in question, the more serious the misconduct and the more severe the likely outcome".*

21.12 The Panel had determined that there was no proper policing purpose for the access.

21.13 The Panel considered the matters set out at paragraph **[4.37]** of the Guidance quoted above and found the following to be applicable namely, that this was a breach of personal privacy where the data is very sensitive.

21.14 The Panel examined paragraphs **[4.10]** and **[4.11]** of the Guidance which are set out below:

[4.10] *"Conduct that is intentional, deliberate, targeted or planned will generally be more culpable than conduct that has unintended consequences, although the consequences of an officer's actions will be relevant to the harm caused".*

[4.11] *"Where harm is unintentional, culpability will be greater if the officer could reasonably have foreseen the risk of harm".*

This was an experienced officer who could reasonably have foreseen the harm of a data breach.

21.15 The Panel assess the level of culpability as High to Medium for a matter of Misconduct.

Harm

21.16 Harm is dealt with in the Guidance from page 27 onwards. It is clear that there are two relevant types of harm: (i) harm to a defined individual; and (ii) harm to the public confidence.

21.17 The Panel considered that it was appropriate to consider the impact of the misconduct on PC A. The Panel had regard to paragraph [4.66] which is set out below:

“Harm will likely undermine public confidence in policing. Harm does not need to be suffered by a defined individual or group to undermine public confidence. Where an officer commits an act that would harm public confidence if the circumstances were known to the public, take this into account. Always take misconduct seriously that undermines discipline and good order within the police service, even if it does not result in harm to individual victims”.

21.18 In addition to the above the Panel noted the Guidance at [4.69]:

“How such behaviour would be, or has been, perceived by the public will be relevant, whether or not the behaviour was known about at the time.”

21.19 Harm does not need to be suffered by a defined individual or group to undermine public confidence. The Panel was satisfied that the facts of this case presented a real risk of reputational damage to the Police and was likely to erode the trust built up over many years and have an adverse impact on the standing and reputation of the profession on the whole as a result. The public rightly have high expectations about how officers conduct themselves and on this occasion the Officer fell well below these expectations.

21.20 There was no deliberate targeting in this case by the officer, but PC A would have been notified of the breach. Common sense dictates that it must have had a negative impact on a person who is a serving officer who has been arrested, with the associated vulnerabilities of someone in that position.

21.21 Having regard to the above the Panel assess the level of harm as High for a matter of misconduct.

Aggravating Factors

21.22 The Panel identified the following aggravating factors:

- Significant deviation from instructions, whether an order, force policy or national guidance. It was also a breach of the Data Protection Act.
- Failure to raise concerns or seek advice from a colleague or senior officer or be as open as she could have been about accessing the record. She did not provide a full explanation or account which the audit process required her to do.

Mitigating Factors

21.23 The Panel identified the following mitigating factors:

- The misconduct was confined to a single episode of brief duration in terms of the access to the data itself.
- There was an acceptance that she was responsible for what had happened and “got it wrong”.

Double Counting

21.24 The Panel have taken care not to double count the aggravating factors with the assessment of culpability and harm set out above and now turn to the assessment of seriousness.

Conclusion on Seriousness

21.25 The Panel considered whether the aggravating/mitigating factors set out above adjusted the level of seriousness identified in this matter in respect of the assessments made in relation to culpability and harm.

21.26 There were some mitigating contextual factors in this case which the Panel set out above.

21.27 However, the Panel concluded that having regard to all the above the level of seriousness for this matter of misconduct did not merit any adjustment and was therefore **at the higher end of the gravity scale for a matter of misconduct**.

Personal Mitigation

21.28 The Panel took note of the Record of Service for the Officer. She was of good character. Several character references were provided and the Panel noted these were very positive. These character references were from a Temporary Chief Superintendent, Chief inspector, 2 former police constable colleagues and a serving police constable. The references all spoke of the professionalism of the Officer. She was described in one reference as being someone who had conducted herself with integrity honesty and reliability. It was noteworthy that since the PSD investigation into this matter had started the Officer had worked in the Prevention Hub where she was described as being a “positive asset” to the team. Another reference described her as being an exemplary officer and an example to others.

The Panel noted her long service and took into account the service history provided.

21.29 The Panel reminded themselves of the dicta of Holroyde J in R (Williams) v Police Appeals Tribunal [2016] EWHC 2708 (Admin) (a case where gross misconduct was found) where he said: *“In my judgment, the importance of maintaining public confidence in and respect for the police service is constant, regardless of the nature of the gross*

misconduct under consideration. What may vary will be the extent to which the particular gross misconduct threatens the preservation of such confidence and respect. The more it does so, the less weight can be given to personal mitigation.”

Stage 2: Purposes of imposing disciplinary action

21.30 The Panel kept in mind the purpose of imposing disciplinary action in police misconduct proceedings namely:

- The primary purpose is to maintain the public confidence in and the reputation of policing;
- The second purpose is the declaratory purpose of maintaining high standards in policing and to deter misconduct;
- The third purpose is to protect the public.

21.31 The Panel concluded that public confidence in policing, and the wider reputation of the service, were an important feature in this case. It also found that the Officer had fallen short of the high standards expected of her, meaning the declaratory purpose of the outcome was engaged. The public is entitled to expect that police forces protect personal data, and the need to safeguard the public was likewise engaged.

Stage 3: Appropriate disciplinary action in this case

21.32 The Panel reminded itself again that misconduct proceedings are not designed to punish police officers – the Panel are essentially concerned with the reputation of the profession rather than punishment.

21.33 The Panel took account of the personal mitigation of the Officer to the extent consistent with case law and the dicta in the case of Williams as set out above.

21.34 The Panel took the view that the personal mitigation offered by the Officer carried some, albeit limited, weight having regard to the fact that what the Officer did could have had a significant detrimental impact on public confidence.

21.35 Having regard to all of the above the Panel concluded that a Written Warning would not be an appropriate sanction bearing in mind the purpose of misconduct proceedings and the assessment of seriousness in this case. In particular, it would not be sufficient to maintain public confidence in the police service and therefore a **Final Written Warning for 2 years** (FWW) was the appropriate and proportionate outcome.

21.36 The Officer has the right of appeal to the Police Appeal Tribunal (PAT).

Publication

21.37. At the conclusion of the hearing the Chair determined that this decision be published subject to redactions to prevent the jigsaw identification of PC A.

ASSISTANT CHIEF OFFICER: RACHEL HARTLAND LANE

INDEPENDENT PANEL MEMBER: DEVIKA ASSI

INDEPENDENT PANEL MEMBER: MARSHA PEARSON

26 FEBRUARY 2026