

IN THE MATTER OF THE POLICE (CONDUCT) REGULATIONS 2020

THE APPROPRIATE AUTHORITY

CHIEF CONSTABLE OF WEST MERCIA

v

PC 22120 CLARKE

PC 22120 Clarke, on 15-16 July 2026 you were asked to appear at a misconduct hearing, which was conducted by:

Chair: DCC Damian Barratt

Independent Panel Member: Jenni Ord

Independent Panel Member: Linda John

Independent Legal Adviser : Harry Ireland

Breach of standard(s) of professional behaviour alleged were as follows:

Alleged Facts

The Appropriate Authority alleges that:

PC 22120 Ryan Clarke (the Officer) joined the West Mercia Police in September 2021.

POLICIES, PROCEDURES AND APPROVED PROFESSIONAL PRACTICES

The College of Policing Approved Professional Practice (the APP) on sharing police information states that,

Sharing police information must be linked to a policing purpose. APP on

information management - management of police information defines such purposes as: - protecting life and property - preserving order - preventing and detecting offences - bringing offenders to justice - any duty or responsibility arising from common or statute law.

All police officers have a duty to ensure that they access information for which they have a legitimate policing purpose.

The West Mercia Data Protection Policy states that:

All personal information is held and processed in accordance with the Data Protection Act 2018. Anyone working within West Mercia Police may only use information in accordance with their Policing duties. 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 purpose(s), it should be noted that the list is in no way exhaustive:-

Any check carried out on behalf of family or friends. 2 The use of Police information systems for a private purpose or any other purpose other than that declared by the Chief Constables to the Information Commissioner is strictly prohibited. Where a member of staff has a personal connection with the other party (e.g victim, witness, suspected offender, offender) they must

declare this connection and the reason for the enquiry/record check to a supervising officer before any action is taken. Details should then be recorded in a pocket notebook if one is issued or via email at the time.

West Mercia Officers had been reminded of the importance of data protection and confidentiality in:

- a. Force orders.
- b. Monthly updates.
- c. PSD inputs.
- d. Training.

In addition, every time a West Mercia police officer signs into a police system they are presented with a declaration that reads as follows:

ATHENA

Athena is a live system. DO NOT USE for any unauthorised activity.

WARNING this is the live Athena system. Use of this system MUST be for a legitimate policing purpose by staff who have been appropriately trained. Staff misusing the system may be liable to prosecution, disciplinary action or both. Do you accept these conditions?

GENIE

Access to police systems is only permitted for official duties and in accordance with the Data Protection Act 1998, other associated legislation and Force Policies and Procedures.

Individuals are only authorised to access, browse, use or disclose personal data in the course of their official duties and for policing purposes only.

Any improper use may leave you liable to criminal or misconduct proceedings

Unless the Officer accepts the conditions set out and acknowledges their individual culpability for use of the systems the Officer cannot access the police systems.

TRAINING

The Officer had received training in relation to data protection and confidentiality on 21 September 2021.

FACTS

In 2021, the Officer was subject to a telephone vetting interview in relation to questions that he had answered on his vetting application. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Accordingly, the Officer was aware that he was required to declare his involvement [REDACTED]

The Officer wrongly accessed confidential information during his role as a police officer.

28 July 2022

The Officer accessed records relating to [REDACTED]. These records included,

e. The fact that he was in custody.

f. His roles.

g. His addresses.

The Officer failed to do the right thing in particular, the Officer failed:

h. To declare the accessing of the data to any supervisor or line-manager or the Professional Standards Department, and/or

i. To declare his connection to [REDACTED] to any supervisor or line-manager or the Professional Standards Department, and/or

j. To record the fact of the access in his pocket notebook, and/or

k. To record the fact of the access in an email or other electronic note

21 and 22 February 2023

The Officer accessed records relating to [REDACTED]. These records included,

l. The fact that he was in custody/his custody record.

m. [REDACTED] image/photograph.

n. His detention log.

The Officer's access was broken into several separate points in time:

o. 12:05 12:06.

p. 12:52 12:54.

q. 13:35 13:37,

And on 22 February:

r. 07:00.

t. 10:12 10:27.

u. 12:24.

v. 13:13.

w. 13:23 13:32.

x. 14:05

The Officer failed to do the right thing in particular, the Officer failed:

y. To declare the accessing of the data to any supervisor or line-manager or the Professional Standards Department, and/or

z. To declare his connection to [REDACTED] to any supervisor or line-manager or e Professional Standards Department, and/or

aa. To record the fact of the access in his pocket notebook, and/or

bb. To record the fact of the access in an email or other electronic note.

PARTICULARS OF MISCONDUCT

Police Constable 22120 Clarke it is alleged that you have breached the Standards of Professional Behaviour, and in particular the standards relating to:

(1) Honesty and Integrity (Integrity only)

In that you acted without integrity, in that you accessed confidential information by virtue of your role for personal reasons and/or when there was no policing purpose so to do as set out at paragraphs 12 -16, and/or you failed to comply with policy and/or to alert the fact of your access to any supervising officer.

(2) Confidentiality

Your behaviour as set out above has breached this Standard.

In that you accessed confidential information by virtue of your role for personal reasons and/or when there was no policing purpose so to do as set out at paragraphs 12 - 16.

(3) Discreditable Conduct

In that your behaviour as set out above has discredited the police service and/or undermined public confidence in it.

It is alleged that these matters individually and/or collectively amount to gross misconduct, namely a breach of the Standards of Professional Behaviour that, if proved, is so serious that your dismissal would be justified.

EVIDENCE

The Panel heard from C and A Rushton (simply to clarify the point as to what C would see when opening the first page on the Genie database). The allegations had been admitted by C but to the level of Misconduct.

C's case remained that whilst he had accessed the police records as alleged, such access, albeit deliberate, was limited and was not utilised in any way. His first access on 28 July 2022 was done whilst undertaking his normal duties. He accessed the Force's intranet which would provide him with information that he was entitled to access and, indeed, would be expected to do so as part of his duties. He saw the surname of [REDACTED] [REDACTED] he accessed the record to establish if it was him. The information seen was nothing that he did not have previous knowledge of. He also accessed the Genie database (which deals with intelligence) but this was limited to the first page. This contained personal details but also listed potential intelligence on links to other criminals etc. Having so established he came out of the system. He acknowledged that he failed to inform anyone about this nor did he make any record of it. He said that he knew that it was 'not the right thing to do.'

The access of the database over the two shifts on 22 and 23 February 2023 followed his seeing [REDACTED] surname again on the 'whiteboard' within the Athena system which lists overnight arrests and detentions. This access was again proper and part of his duties on beginning his shift. He then accessed [REDACTED] record on several occasions over the next 2 days. C was concerned as he [REDACTED] thought that [REDACTED] had changed his ways and gone on 'the straight and narrow.' He acknowledged that in accessing the records he was acting improperly. He made no note of his actions. He claimed that he recollected informing a sergeant of his actions but could not identify who. Enquires by the AA could not establish any of the likely sergeants being so informed. His 'hovering' over [REDACTED] photograph he thinks was as a result of locking his laptop whilst the cursor was still on the photograph. He did not need to keep viewing this.

He admitted that he had accessed the custody record and detention log which covered pages 68 – 95 in the bundle. He said that he was 'curious' because [REDACTED] was still in custody from the previous day.. He conceded that if he had gone to the custody suite and asked the custody sergeant if he could view the logs he would be told to go away. He claimed that because

he was dealing with two offenders accused of theft that afternoon, he had little time to spend time looking at [REDACTED] records. The access at 13:23 on 23 February shows that he spent over 4 minutes reading them. The records would contain information relating to reasons for arrest and detention as well as any interventions he required. Thus, inevitably sensitive information was accessed by C. Again, he admitted that he had made no record of this.

In cross examination he accepted that in seeking to join the police, he had declared the fact that [REDACTED] had been in trouble and as a result of this, his training and a subsequent vetting conversation, he was fully aware of his duties and responsibilities in relation to sensitive information and accessing the same. He accepted that his obligations were clear. He failed to inform any line manager or make any record of the 3 occasions he accessed the database and accepted that curiosity was not a valid reason for such access. The Panel did not accept his reason for his failure to inform any supervisor of such access based on embarrassment or lack of confidence as he told the Panel of other instances where he had informed a supervisor of negative actions, e.g. when he had caused minor damage to a police vehicle. Similarly, the Panel could find no reason for his failure to record his actions given the fact that he told the Panel that he kept his pocket notebook up to date 'religiously.' He also accepted that given the [REDACTED] he should, having seen it, not gone any further other than to inform his supervisor of the possible relationship. In dealing with his assertion that he had informed an unnamed sergeant of his access to the database, he conceded that it was more likely than not that he had not done so, as any such report would have led to an audit trail.

In determining the level of misconduct, the Panel took into account the following factors:

1. C had accepted that he had deliberately accessed police database records that he should not have done, had not informed any supervisor of his actions nor made any record of his actions. It also accepted the proposition advanced on behalf of the AA that C's culpability increased with each occasion he accessed the information; it was not an isolated incident and there were several months separating the first and then the second and third occasions.

2. That in accessing such information there was the potential for not only viewing sensitive intelligence data but also compromising the same. This was balanced by the fact that the Panel accepted that C's access was limited and there was no evidence that it had been relayed to any other person. Nevertheless there was a risk to the police, (and others should sensitive information be passed on), with C placing himself in a potentially vulnerable position.

3. C had undertaken the access of the police database despite his experiences relating to [REDACTED] when joining the police and that he knew his actions were wrong.

4. C's actions were both deliberate and intentional and the seriousness increased with each occasion.

5. The Panel noted the College of Police Guidance on Outcomes regarding such misconduct where it states the following:

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.

In considering such guidance, the Panel accepted the submissions made on behalf of C that none of the aggravating factors specified in paragraph 4.37 existed and therefore accepted that this was not in the category of the most serious cases.

6. The Panel accepted the AA's submission that the actions of C were akin to a criminal offence under s170 Data Protection Act 2018.

7. The harm occasioned by C's actions is the detrimental effect on public confidence where police officers access personal often sensitive information for improper purposes (including curiosity). In other professions the impact on the public have shown to be potentially devastating (e.g as in the recent Nottingham Health Authority case) and such breaches may severely undermine public confidence. However, the Panel balanced this by accepting C's evidence that the information he accessed purely related to [REDACTED] and most of the information seen would be within his existing knowledge (save for detail contained within the Custody Record and Detention Log). Accordingly public confidence if all the facts were known, would be harmed but not to a significant degree.

8. The Panel therefore found that C's culpability to be high and the harm caused to be medium.

The Panel concluded that C breached the Standards of Professional Behaviour in relation to Honesty and Integrity (Integrity only), Confidentiality and Discreditable Conduct and such breaches amount to Gross Misconduct.

CONCLUSION

The purpose of the misconduct hearing is threefold:

Firstly, to protect the public confidence in and the reputation of policing.

Secondly, to maintain the high professional standards by demonstrating to other officers that misconduct will not be tolerated.

Thirdly, to protect the public and/or officers and staff by preventing the officers from committing similar misconduct again.

In determining the appropriate sanction, we took into account the following matters:

CULPABILITY

The Panel being aware of the need to avoid double counting, simply relied on those factors identified when assessing the level of misconduct as recorded above.

HARM

The Panel noted the submissions on behalf of the AA regarding risk when considering the issue of harm and agreed with the principle advanced, but such risk must be realistic and not fanciful. However, the Panel considered carefully the actions of C and the level of information he accessed. From this the Panel concluded that any risk was to [REDACTED] having personal data published as well as a risk to C's vulnerability to undue influence. However, the greatest risk, as identified above, is the risk of the adverse impact on public confidence and their trust in the police holding personal data securely.

AGGRAVATING FACTORS.

C had concealed his wrongdoing both by failing to report his actions to a supervisor and failing to record the same.

The conduct was repeated over a period of months.

C continued with his behaviour when he knew it was wrong. He admitted that he knew this to be the case when engaging on his first access in July 2022 but continued doing this twice more in February 2023.

C's actions significantly deviated from instructions and Force policy.

There were multiple allegations.

MITIGATING FACTORS

C made admissions at an early stage but given the overwhelming nature of the evidence against him, any credit must be limited, especially as it was not a full and frank admission (e.g. claiming that he thought that he had told an unnamed sergeant of his access).

There was evidence of remorse and insight as to his wrongdoing.

The Panel noted the character references submitted on C's behalf. It was noted that C had worked well to a good standard and without any sickness absence during the misconduct process. It is to C's credit that he obtained his policing degree during this time.

OUTCOME

As directed in the Guidance, the Panel began with the least punitive option.

The only possible alternative to dismissal was a Final Written Warning, of whatever length.

The Panel found that given the 3 aims of the regime as identified above, public confidence in the police's ability to handle private and sensitive information securely is paramount. It is vital for public trust. The Panel noted that C was an inexperienced officer at the time of the events complained of, and his access of data was limited as described above.

The Panel found that the imposition of a Final Written Warning would not meet the aims of the regime and would not be sufficient to maintain public confidence particularly in relation to the handling of personal data, especially with an officer accessing such data on three separate occasions. Nor would, the Panel found, it act as a sufficient deterrent to others who may be tempted to access private information simply to satisfy their curiosity.

Accordingly, the only appropriate sanction that is appropriate is Dismissal without Notice.