Witness Name: KATHRYN CRANER

Statement No: WITN0044001

Dated: 5 December 2025

THE NOTTINGHAM INQUIRY

FIRST WITNESS STATEMENT OF SUPERINTENDENT KATHRYN CRANER

I, KATHRYN CRANER, will say as follows: -

1. My name is Kathryn Craner.
2. This witness statement is made to assist the Nottingham Inquiry (the "**Inquiry**") with the matters set out in the Rule 9(3) Request dated 3rd June 2025 (the "**Request**").

My Background

3. Prior to joining the police, I obtained a BA Geography degree and following this, having worked to save money, I travelled to Ghana where I taught English in a secondary school as a volunteer. I joined Nottinghamshire Police on 1st October 2001 and after passing through the ranks I was promoted to substantive Superintendent on 28th February 2022 in the posting of City Commander.
4. On 1 March 2024 I became the Head of the Professional Standards Directorate ("PSD") for Nottinghamshire Police. My department consists of the Complaints and Misconduct Unit, the Counter-Corruption Unit ("CCU") and the Vetting Unit.

5. On behalf of Nottinghamshire Police, I am the appropriate person to address this Rule 9 request because my professional portfolio concerns allegations of misconduct against police officers and staff.

The units within PSD

6. The CCU focuses on the prevention, detection and investigation of corrupt practices involving officers and staff within Nottinghamshire Police. The CCU's functions include:
   a. Using covert tactics to monitor signs of corruption;
   b. Implementing policies and training to reduce opportunities for misconduct;
   c. Investigating allegations and intelligence taking disciplinary or criminal action where necessary. The CCU have responsibility for the policing of and response to unauthorised access and disclosure of information.
7. The Complaints and Misconduct Unit's functions include:
   a. Handling public complaints under the Police Reform Act 2002 ("PRA");
   b. Reactive investigation into allegation of misconduct whether under the PRA or Police (Conduct) Regulations 2020;
   c. Presenting cases of misconduct to meetings or panels.
8. The Force Vetting Unit is responsible for undertaking all aspects of police and non-police personnel vetting, delivering the expectations set out in the Vetting Code of Practice and compliance with the standards detailed in the Vetting Authorised Professional Practice and The Police (Vetting) Regulations 2025. It is the Unit's responsibility to:-
   a. Assess the suitability of individuals for roles that grant access to police information, systems, or premises, ensuring they meet the ethical and

professional standards expected in policing and pose no risk to the public and to those who are particularly vulnerable.

b. Identify and manage risks including corruption, coercion, misconduct, or vulnerability. This includes evaluating criminal history, financial status, and personal associations.

c. Undertake continuous monitoring and reassessment of individuals when there is a material change in circumstances, such as misconduct allegations, financial difficulties or changes in circumstances, to ensure they still meet the required standards.

Timing of sensitive data, information and/or CCTV footage in respect of this high-profile case coming into the possession or access of Nottinghamshire Police (officers and staff)

9. The volume of information and material generated as a result of Valdo Calocane's attacks is significant. This would include, but is not limited to, phone calls, incident logs, crime reports, CCTV, Body Worn Video, Crime Scene Investigator logs, officer statements, witness statements, expert statements, case file material, custody material.

10. From the time of the first reports being received by Nottinghamshire Police on the 13th June 2023, information was being continually added to the various crime recording and management systems and databases operated by the Force.

11. Crime occurrences were created on our NICHE system. NICHE is an IT platform which incorporates crime, intelligence, custody and case management information linked to a "Golden Nominal" record. A Golden Nominal is the master record for an individual. It links all aliases, addresses, identifiers (like

fingerprints or DNA), and interactions with police into one unified profile. It allows officers and analysts to get a complete picture of a person's history, associations, and risk level. It supports intelligence-led policing, safeguarding, and case management. NICHE access is provided to all officers and staff whose roles require it.

12. Anyone with relevant material, such as a statement, would store it on this system. Every crime recorded as a result of the events of 13th June 2023 would be created as a unique occurrence, however, there can sometimes be overlapping evidence for more than one crime. It is common in this situation for one to be selected as a 'master' occurrence to ensure that the investigating officer can see all material within one record. I can see from the NICHE 'master' crime report reference 23000363440 that there are 128 different documents on there, including statements, use of force forms, photograph exhibits and sudden death reports.

13. The Major Crime Unit, which led the investigation into the 13th June 2023 attacks, utilised the Home Office Large Major Enquiry System ("HOLMES") to manage and investigate the crimes and evidential material would be stored on this system and actions would be generated. Only those officers and staff who had a HOLMES account would be able to access the material on this system.

14. Each enquiry run on HOLMES is a separate self-contained database. The database for this enquiry was given the operational name 'Operation Hendrix' (operational names are randomly generated). All individuals working on the enquiry had to be given access to that database before they could log onto it. Therefore, not everyone who has access to HOLMES would have access to the database containing the material for Operation Hendrix. Additionally, there are

different access levels within each database, so that, for example, if a document was marked as 'sensitive' then access to it would be restricted to users with that access level allocated to them.

15. The HOLMES account for Operation Hendrix was created on the morning of 13th June 2023. The HOLMES staff (or file officer) went through the NICHE occurrence(s) and duplicated all the documents that had already been submitted (for example by Response officers, Crime Scene Investigators etc.) and submitted them to the HOLMES account. This ensured that all information was logged and reviewed within HOLMES. Each document in NICHE was marked 'submitted to HOLMES' with the date of submission, in order to ensure that all material had been moved.

16. Once an enquiry is placed on HOLMES, officers and staff submit all subsequently created documentation into HOLMES. However, some documents would also need to be created on NICHE in order to facilitate the creation of a Case File for submission to the Crown Prosecution Service (CPS) via NICHE.

17. Body Worn Video is stored on a system called NICE Investigate. This is a Digital Evidence Management System ("DEMS") and is designed to create a single repository for the storage and sharing of digital evidence collected in an investigation.

18. The NICE Investigate system is also used to store any CCTV obtained during the course of the investigation and other digital material. The material is organised according to the NICHE crime reference. I can see that there are 420 items under what was designated as the master crime reference (23000360085).

Nottinghamshire Police guidance on the holding and viewing of sensitive data, information or material

19. I would like to clarify that I have assumed the Public Inquiry to be referring to "sensitive" in the wider and more generic sense rather than the definition applied under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

20. Nottinghamshire Police strives to provide guidance and training to try to ensure that its officers and staff are well-informed about the holding, handling and viewing of police data, information or material. I will set out the policies first:

21. The Acceptable Use Policy and Generic Security Operating Policy (SyOps) for all Police Information Systems (PS 163) (NGPF0007438) is owned by the Information Management Lead. This policy defines the acceptable use of Police Information systems and applies to all police officers and police staff, including members of partner agencies who require access to some part of police systems to enable joint working and those working voluntarily or under contract to the police (agency workers, contractors and third parties with access to Police information assets).

22. This policy states at paragraph 2.3 "You are only authorised to access, browse, use, or disclose Police information in the course of your official duties and for policing/business purposes only."

23. At paragraph 2.2 'Policing Purposes' are defined as:

    a. Prevention and detection of crime

    b. Apprehension and prosecution of offenders

    c. Protection of life and property

d. Maintenance of law and order

e. Assisting the public in accordance with Force policies and procedures.

24. At paragraph 2.9 this policy states: "In order to ensure that the above standards are met, the information and communication systems that you use can be recorded or monitored. Consequently, there can be no expectation of privacy in the use of any information or communication facility provided by the Police."

25. The policy confirms at paragraph 16.1 that "Individuals who abuse or misuse systems will be liable to one or more of the following sanctions:

a) Denial or restriction of access to Police systems and facilities;

b) Disciplinary action;

c) Criminal proceedings."

26. Every time a user logs onto the Nottinghamshire Police system the log in screen sets out the terms and conditions for use of that system which are explicit that they may only access or use Nottinghamshire Police systems and information for business purposes. It reminds them of the definition of a 'policing purpose' and they must click to accept that they agree to the terms and conditions, as follows:

27. "By entering this site you are accepting and agreeing to adhere to Nottinghamshire Police Standards & Policy.

1) You may only access or use Nottinghamshire Police systems and information for business purposes – this includes e-mail, Internet/intranet and all IT applications that are accessible via the Force's IT network or other Force computers and systems, including by way of mobile devices and telephones.

2) Policing information – As per APP Information Management; Police information refers to all information obtained, recorded or processed for a

policing purpose. A policing/law enforcement purpose is defined in Part 3: Sec 31 of the Data Protection Act 2018 as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3) Non-Policing Information; Is defined as any Nottinghamshire Police owned information used for non-policing purposes, for example Employment, Finance & Corporate Governance purposes, this may also include personal data that is processed under Part 2 of the General Data Protection Regulations (GDPR).

4) The acceptable use of Nottinghamshire Police information and assets is detailed in PS 163 Acceptable Use Policy.

5) In order to ensure compliance with relevant legislation and Force policy, the information and communication systems that you use may be recorded or monitored (as PS 310 Lawful Business Monitoring Policy).

6) Consequently, there can be no expectation of privacy in the use of any information or communication facility provided by Nottinghamshire Police.

7) Please note: You have an individual responsibility to ensure that all information Assets you process are managed securely and in line with relevant legislation, policy & standards. This responsibility applies to every role, every rank and grade and in every part of this organisation and its partner agencies. Individuals can be liable under civil and criminal law and may face disciplinary action and prosecution where information is processed outside of these and without proper authority.

28. When logging onto the NICE system users are faced with an additional warning which they must accept before being allowed access. This reads as follows:

28. "Restricted information system. Unauthorised access is strictly forbidden and is a disciplinary offence. This system contains RESTRICTED information. You may only access this system if you are authorised to do so by your Force and only for the purpose of that authorisation. The information contained within is for policing purposes only. The Policing Purpose is described as the prevention and detection of crime, apprehension and prosecution of offenders, protection of life and property, maintenance of law and order and rendering assistance to the public in accordance with your Force policies and procedure. DO NOT let others use your log on. Use of this system is audited and therefore you should have no expectations of privacy. Any misuse, including searching for your own personal purposes of curiosity, may result in criminal and/or disciplinary proceedings. By accessing the system, you fully accept that you understand and comply with all Force policies and legislation."

29. When logging onto the Niche system users are faced with an additional warning and reminder which they must accept before being allowed access. This reads as follows:

30. "IMPORTANT NOTICE: DATA PROTECTION ACT 2018, GENERAL DATA PROTECTION REGULATION (EU Regulation 2016/679), THE COMPUTER MISUSE ACT 1990. Police Officers, Police and Partnership Staff, Contractors and Volunteers are reminded that this system and the information held within it are subject to the above Acts. Unauthorised access to the system or parts of the system and/or unauthorised disclosure of personal information from the system could result in severe penalties, including possible criminal prosecution and/or proceedings under the disciplinary code. By proceeding you confirm that you are aware of your obligations as defined in the force Information Security

Policy and the force Data Protection Policy. You are also reminded that any access to information held on Police information systems including externally managed systems such as PNC and PND should be accessed only for a policing purpose and NOT for curiosity. All officers and Staff must be aware at all times of who can view their screen before logging on and accessing data. All Officers and Staff must also be aware of who they are sharing data with and that there is a legitimate reason to do so."

31. Nottinghamshire Police provides relevant training for all new starters into the force: officers, specials and police staff. This training is conducted at Nottinghamshire Police Training School by a dedicated training team complemented by guest speakers. A mandatory lesson within the training package for any new starter is about standards and expectations within the police and this includes an explanation of policies and procedures such as the Acceptable Use Policy. I have been able to access the PSD drive and have identified examples of PowerPoint presentations. I can see these dating back to 2021. I exhibit a copy of the slide which supports the presentation on misuse of information as NGPF0007882.

32. Since January 2020, the Professional Standards Department has been delivering in person inputs to all new officers and staff joining Nottinghamshire Police to ensure they are aware of expectations relating to the Standards of Professional Behaviour. This covers all relevant policies and procedures, including the expectations regarding Disclosure of Information and Misuse of Police Systems. In addition to face-to-face learning, all new starters (officers and staff) in Nottinghamshire Police are required to complete mandatory e-Learning Packages including the following modules: 'Counter Corruption',

'Protecting Information', 'Managing Information Operational' and 'Managing Information Operational Challenges', 'An Introduction to Government Security Classification (GSC)' and 'Protecting Information'.

33. E-Learning is short for electronic learning and refers to education or training delivered digitally, typically via the internet or a computer network.

34. Nottinghamshire Police mandate e-Learning packages each month through the Training Priorities Panel. This is in addition to face-to face learning. All officers and staff are required to complete the mandatory e-learning. Completion of mandatory packages is monitored and those who do not complete the package are first sent e-mail reminders and then, if the package has still not been completed, the non-compliance is escalated through line management i.e. first line manager, second line manager and finally Head of Department.

35. There are annual reminders to the workforce about their responsibilities in relation to the 'Acceptable use of Force Systems' policy. In June 2023, these discussions occurred during the annual Career Conversation. The Career Conversation is a formal annual discussion between the individual and their line manager. The Career Conversation is a two-way process, more commonly known as Personal Development Review. It is focussed on an individual's welfare, career aspirations, personal development, performance and opportunities. It should be a meaningful discussion where performance over the previous 12 months and achievements against set objectives are reviewed in an open discussion and future objectives are clearly set against organisational requirements and identified personal development needs.

36. Within the Career Conversation is the Integrity Health Check where line managers must specifically go through each question to complete the check

following discussion with the individual. The form directs the line manager to check the individual has either completed or is aware of the requirements in each category and to take any appropriate action.

37. This Integrity Health Check includes the requirement for a line manager to ensure the individual understands the requirements for the acceptable use of force systems. Compliance with the completion of the Career Conversation is monitored monthly across the force and reported via the monthly Workforce Planning paper to the Force Executive Board chaired by the Chief Constable. Completion rates are also shared more locally at Senior Leadership team meetings and individuals who had failed to complete their Career Conversation were repeatedly chased for this.

38. In addition to guidance through training and policy, Nottinghamshire Police also aims to deter by publicising enforcement of the policy when officers or staff have accessed information without authority or misused information.

39. The 'Misconduct and Criminality Communications Policy' NGPF0007451 was introduced in January 2016 and reviewed regularly. Version 5.0 is dated June 2023. The policy states "To demonstrate that the Force upholds these values and to maintain public confidence in Nottinghamshire Police, the Force must take a consistent, lawful and corporate stance to how we communicate on those occasions when officers or staff are suspected of falling short of our values and standards and face misconduct or criminal proceedings as a result."

40. Under the section relating to 'Misconduct Outcomes – Officers' it states the following: "There will need to be allowance made at the hearing for representations in relation to the publication of the outcome. These will likely be made in respect of the initial misconduct hearing notice as there is no

requirement to seek further representations post hearing. At the discretion of the hearing Chair, the outcome notice will be prepared by Corporate Communication and may contain the following information:

a) The individual's name, role and place of work / base

b) Details of the misconduct as set out in the reg 21 notice

c) The finding of the panel

d) Any disciplinary sanction imposed"

41. It further states "The Force recognises the Regulation guidance that the outcome notice should be published on the Force's website not before seven and not later than 12 working days after the hearing and remain on the website for a minimum period of 28 days. However, at the discretion of the hearing Chair and to ensure transparency, the timeliness of publication may be considered against other factors such as whether the hearing has been in public, whether media have attended and if there is significant public interest. The same notice, or a variation of, as outlined by the hearing Chair, will also appear on the Force's Intranet page."

42. I have caused the PSD Centurion case management system to be searched to identify cases where individuals have proceeded to a Gross Misconduct proceeding for allegations relating to accessing systems without a policing purpose. My request was to identify such matters where the date of the hearing was between January 2020 and June 2023. There were 9 cases identified on the system which progressed to a hearing. Of these, 8 officers were dismissed and 1 was given a final written warning.

43. I believe that the workforce would have been reminded through either articles or commentary within the workforce that it was not acceptable to view material other than for a policing purpose.

Steps taken in this case to ensure that information generated as a result of the events of 13 June was restricted only to those with a legitimate need for access

44. Access to material generated by an investigation and stored on any Nottinghamshire Police systems can be restricted. This would mean that only designated individuals would be able to view the content. This can be applied to NICHE incidents, SAFE Command and Control incidents and NICE Investigate.

45. I have identified policy PS 295 Restricted incidents and Authorised Access NGPF0007442. This is owned by Contact Management and was in place in June 2023. It states that "The aims of this policy are to provide:

- Clear guidelines to the criteria for restricting an incident;
- Authorizing access to restricted incidents;
- On-going management of restricted incidents; and
- Organisational compliance."

46. The policy states that "the following incident restriction criteria has been agreed for either immediate or 'as soon as operationally practicable' restriction:

- Kidnap & Extortion – excluding Honour Based Violence (HBV) incidents;

• Risk to national security;

• Any incident containing source information;

• Any incident involving covert tactics."

47. It goes on to state that the "following incident types have been agreed for restricting in the first instance, however the restriction will be removed at point of closure or as soon as practicable afterwards following review by the Officer In Charge (OIC):

• Any incident whereby Post Incident Management (PIM) is commenced;

• Live on-going incidents of a sensitive nature (restriction to be lifted once the initial incident is closed); and

• Any incident involving an off duty staff member where offences are being alleged against them."

48. The policy goes onto explain that some roles will automatically be given access to a restricted incident should this be requested, but that any other individuals requiring access would need to have this granted by the Control Room Chief Inspector, Control Room Sergeant or Control Room Supervisors.

49. There is also guidance available to explain how NICHE occurrences can be restricted. This provides the primary options for restriction as follows:

- Relates to National Security
- Involves current member of police staff or police officer involved in murder, manslaughter or rape

50. It then provides an additional seven options for restriction of the occurrence with each then requiring a full explanation and rationale:

- Protect the source of subject from harm
- Protect any other person, to whom the information impacts, from harm
- Protect the integrity of a sensitive policing operation or activity
- Prevent the deliberate or accidental leaking of sensitive information to non-authorised personnel
- Reduce the risk of compromise to a criminal / disciplinary investigation
- Protect the privacy of the subject (balanced against potential harm caused by failure to share)
- Other (please specify)

51. The guidance states that an officer of the rank of Inspector or above is the decision maker as to whether to restrict an occurrence.

52. The NICE Investigate system allows for access to be restricted. There are no published criteria for when to consider restricting a file. Restriction can only be applied to the whole file, not parts, and means that no-one else would be able to see the material contained within it. The system allows the individual who has restricted access to permit others to have access by listing them individually.

53. The material generated following the events of 13th June 2023 was predominantly held on the SAFE Command and Control system, NICHE, NICE Investigate and HOLMES.

54. Incident 77_13062023 was restricted at 17:32 hours on the 21st June 2023. This was in belated recognition that the criteria relating to the calling of a Post Incident Management had been met.

55. No other restrictions were put in place. It would have been possible to restrict the occurrences in Niche though in my opinion that would have significantly hindered the investigation or would have required a team of people dedicated to giving access to individuals as and when required.

56. For an officer or staff member to add a witness statement to NICHE (whether their own statement or a statement taken from another person) it is necessary to access the NICHE occurrence and attach the document. If access has been restricted, access would have to be sought from an administrator each time. This would have been bureaucratic and time-consuming and injurious to the efficiency of the investigation.

57. Intelligence reports are also added to NICHE and then linked to either a nominal, an address or a vehicle. Restricting access would risk important information being missed.

58. Crime Scene Investigators add their reports through the Occurrence onto NICHE. If access has been restricted, access would have to be sought from an administrator each time, again adding administrative bureaucracy.

59. All exhibits are booked onto NICHE and linked to the Occurrence. It is possible to use a Nottinghamshire Police webform to list the items of property and their exhibit references, but it would not be possible to then link the exhibits to NICHE without access to the occurrence. If access has been restricted, access would have to be sought from an administrator each time.

60. The NICHE occurrence is utilised to submit items for Forensic examination, If access has been restricted, access would have to be sought from an administrator each time.

61. The Case File for submission to the Crown Prosecution Service is created on NICHE. This function links all the crime occurrences which are the subject of the proposed charge into a Casefile, along with the associated case file documentation, and then interfaces with the Crown Prosecution Service to enable a two-way sharing of information and documentation. If access has been restricted, access would have to be sought from an administrator by the Crown Prosecution Service lawyers.

62. The crime occurrences also have to be linked to the Custody Record because this information is used to populate the Police National Computer for the subject of an investigation.

63. In summary, I believe that restricting one or more of the occurrences would have created significant logistical challenges for Nottinghamshire Police and in tension with the objective of effectively and expeditiously investigating the crimes to reach a successful charge within the time constraints of Police and Criminal Evidence Act 1984.

64. The NICE Investigate system does not allow individual exhibits to be restricted; it will only allow the entire master record for the crime to be restricted. Due to the volume of people working on the investigation this would have been logistically challenging with individuals having to request access to the record. As with NICHE, if the master record is restricted then no-one else can view it or search for it.

65. It was essential to store all digital exhibits in one location to enable the Major Crime enquiry team to access and review the relevant material.

66. At the second meeting of the Operation Hendrix Gold Command group on the 14th June 2023, the minutes (NGPF0004863) show that Detective

Superintendent Williams, the then Head of PSD, raised the following item: "HW stated that PSD had been receiving referrals from departments saying that members of staff not involved in the incident had been reading the incident on the system. There is no time to audit all checks on the system, therefore she asked that Heads of Department remind staff and officers that they must have a policing purpose for looking at the incident/CCTV and must not do so if they do not have one. HW went on to say that Inspectors will be asked to deal with it if it is a one off and that if there is anything more intrusive it will be dealt with by PSD."

67. The Gold Group chair, Assistant Chief Constable Griffin set the following action "ACTION: Det Ch Supt Scurr/Ch Supt Verma and Ch Supt Lawton to feed through to their commands that officers and staff must not look at the incident or view the CCTV unless they have a lawful purpose." This action was discharged with updates that these messages had been cascaded.

68. At 09:53 hours on 14th June 2023 Detective Inspector Harding of PSD requested a message be drafted reminding personnel within Nottinghamshire Police not to look at systems without a proper policing purpose and that individual Inspectors could deal with anyone on their team who they believed had inappropriately looked at the incident. DI Harding noted that a lot of self-briefing would have been taking place in anticipation of deployment and establishing who had and had not had legitimate access would be difficult at that time. I refer to this email as police item (NGPF0007863)

69. DI Harding also stated that he understood that on the night all officers in the County were directed to the City so an audit of the incident would be significant, and many officers might not have been shown on the incident as in attendance

(when they were) and so establishing who had and had not had legitimate access would be difficult. As a result, it was decided not to audit the incident or identify which employees viewed it.

70. The minutes from the Gold group indicate that ACC Griffin was in agreement with this position, and as a result, provided the action (noted in paragraph 67) to his senior leaders.

71. The context missing was the significant impact the investigation was placing on resources of Nottinghamshire Police, just over 24 hours after the attacks, including PSD. Therefore, I believe that the initial decision not to audit those who had viewed the incident was correct and was justifiably influenced by considerations of capacity.

72. However, in hindsight, I believe that there should have been a differentiation between viewing the incident log and viewing any CCTV as mentioned in the update to the Gold group, where the reminder proposed by D/Superintendent Williams related to viewing the incident and viewing CCTV.

73. In addition, I believe that DI Harding raised a matter which I believe should be addressed, that of self-briefing. Again, I caveat on this occasion against the huge volume of resources of Nottinghamshire Police to enable the investigation to progress. It is my recollection that there were 60 people required to cover the scenes alone, most of which remained in place for the majority of the 13th June 2023.

74. However, I do believe that if a supervisor was requesting a member of their team to 'self-brief' either because they were being deployed to the investigation or they were potentially going to be deployed, that they should set clear

parameters over the material that they are to access. This would remove any ambiguity around whether this was being accessed for a policing purpose.

75. At the Gold Group meeting of the 20th June 2023, the minutes NGPF0004635 record that Detective Superintendent Williams provided the following update: "HW reiterated that people should not look at incidents/CCTV on systems if they are not directly connected to the job. She asked that this be reinforced to staff forcewide as curiosity is not an excuse and the family trust/confidence must be maintained. RG [ACC Rob Griffin] stated that he had hoped that this was clear to people from the outset but that the message does not appear to have been adhered to. He went on to say that far too many people had made unnecessary checks and stressed the need for teams to be reminded."

76. Detective Superintendent Williams continued in those minutes: "HW stated that the Federation and Staff Associations would also put out a reminder in conjunction with herself and that there may be people within that category that have watched the CCTV without a legitimate purpose and now feel that they cannot ask for support. She went on to say that a form of words would be developed around amnesty of responsibility in this case. People should be directed to their own SMT (Senior Management Team) initially for an assessment and anyone making multiple unwarranted checks should be referred to PSD. HW stated that it was important however that those that needed support should get it, but that those that have shared information will get no amnesty at all."

77. During this Gold Group meeting ACC Griffin set the following action: "Det Supt Williams, in conjunction with the Federation/Staff Associations to provide a form

of words for a comms message around viewing the Op Hendrix CCTV without a policing purpose and associated trauma."

78. The Gold Group minutes dated 20th June 2023 state: "A discussion was held with regards to whether restrictions could be placed on incidents such as this from the outset to actively prevent people looking at them without a policing purpose. RG stated that, he took the point but did not want to stray down that path. He went on to say that, if we arrive at a time in policing where it is felt that there is a need to start restricting normal incidents, (but in this case one that requires an extraordinary response), to certain people to protect them from themselves things have gone badly wrong. There is a need to keep impressing upon people, as senior leaders, the type of culture that we want and that people should know when the [sic] can look at an incident and when they cannot."

79. On 22nd June 2023, a message was sent to the email address of every person in Nottinghamshire Police with an email account setting out the expectations in relation to accessing and viewing material without a policing purpose in relation to this investigation. I refer to this as police item NGPF0007866

80. In conclusion, I can state that restricting information in relation to this inquiry would have created significant logistical challenges for the investigation team and that a decision was made by ACC Griffin not to restrict access to systems. ACC Griffin directed that messages be shared, both by cascading through line managers, and then directly via email, to remind people not to access information without a policing purpose.

Numbers of people within Nottinghamshire Police who accessed sensitive data, information or material held, and/or referred to it in inappropriate telephone messaging with others

81. Whilst the Information Management Unit have responsibility and ownership for The Acceptable Use Policy and Generic Security Operating Policy (PS 163) as previously referred to, it is the Professional Standards Directorate who have oversight and responsibility for dealing with breaches of policy and therefore I have accessed PSD systems to assist me in answering this question.

82. I have assumed this question is directed at sensitive data, information or material held with respect to the attacks of the 13th June 2023. I have reviewed information from PSD systems to understand the timeline and decision making of PSD involvement in this investigation. I have reviewed a summary of the work undertaken by PSD to investigate and deal with unauthorised access to information entitled 'CCU activity – Op Glint (subjects where formal action taken).' I will refer to this as NGPF0005638 . I have also reviewed minutes from Operation Hendrix Gold Group meetings to support my understanding of events.

83. I have caused PSD systems and mailboxes to be checked and have only identified one email received into the PSD inbox which correlates to the information provided by Detective Superintendent Williams to the Gold group on 14th June 2023. This was received at 09:22 hours on 14th June 2023 and located under reference MI/441/23 NGPF0007865 This is a message from a Neighbourhood Policing Inspector to the PSD internal inbox, stating that it had come to her attention that a police officer on her team had viewed the incident

log for the 'Op Plato' incident on 13th June 2023. Whilst not specifically referenced, I would interpret this to be incident 0077_13062023.

84. Operation Plato is the UK police's nationally recognised response plan for dealing with a marauding terrorist attack ("MTA")—an incident where attackers move through a location aiming to kill or injure as many people as possible, often using firearms, bladed weapons, or vehicles. Nottinghamshire Police declared the incident as Op Plato when Valdo Calocane had used a vehicle to attack 3 members of the public.

85. I can see that this PSD referral was reviewed by the PSD Detective Sergeant (DS) (now Detective Inspector) Louise Bradford who forwarded the email NGPF0007865 to D/Supt Williams, DCI Reynolds, Detective Inspector (DI) Gareth Harding (now DCI Harding) and DS Steve King. They formed the PSD senior leadership team at this time. DS Bradford proposed that the matter be dealt with by the line manager discussing the policing purpose with the individual.

86. This decision was ratified by the PSD Detective Inspector Gareth Harding and was the position adopted by D/Superintendent Williams when she attended the Gold group of 14th June 2023 with subsequent action set by ACC Griffin as described in paragraph 67 of this statement.

87. On the 16th June 2023 Detective Superintendent Williams received information from the Chief Officer Team suggesting that there had been a disclosure of highly sensitive information by persons unknown (but by assumption, an individual with access to Nottinghamshire Police systems) to unknown persons in the media relating to Calocane. The information was that Calocane was wanted on warrant and had previously attended a location linked to MI5. These

concerns had been raised to the Chief Officer Team by the Media team. I have spoken to Chief Constable Steven Cooper, and he recollects that he raised the issue with D/Supt Williams as a result of information he saw in the media which he knew had not been provided by Nottinghamshire Police. The subsequent Lawful Business Monitoring activity was recorded on Clue reference 1557 NGPF0005639 and Centurion reference CM/49/23. Clue is the system used to record CCU activity and updates.

88. Within Clue reference 1557 the first update is on 17th June 2023 at 16:25 with an entry from DI Harding. He states: "It is important to note that at present there is no intelligence that the leakage of information has been from a Police Officer or staff member. It will be important to assess each concern and determine who was aware of the information. For example, it is likely that information will have been shared verbally at Gold Group meetings. Similarly, it is also relevant that there were a number of witnesses to the offences who will have seen first-hand the events being reported and could provide the information to the media. This has already been seen in the case with the CCTV of the suspect attempting to access the hostel being provided to the media. At present I propose that this investigation starts by looking at the email created by Det Supt Williams and provided to ACC Griffin. This contained some of the information that has been enquired about by the media including that the suspect was outstanding for an FTA warrant and had previously been arrested for assault on a flat mate."

89. I exhibit the e-mail created by D/Superintendent Williams and provided to ACC Griffin (as referenced above) NGPF0005854.

90. DI Harding decided to commence Lawful Business Monitoring on 17th June 2023, by auditing those who had viewed the NICHE nominal record of Valdo

Calocane. DI Harding recorded: "The systems audits are authorised under the LBM policy as a reasonable and proportionate line of enquiry to prove or disprove the intelligence, safeguard the information held by Nottinghamshire Police and identify any misconduct / criminal allegations. The allegations if proven would likely result in at least misconduct and could constitute criminal offences (MIPO, S26 Corruption[1], DPA offences, etc). The audits will be commenced with the least intrusive available and expanded where required." This activity was recorded under the name Operation Glint.

PC Gell

91. Initial audit scoping was carried out by CCU DC Lee Keeling between 08:00 and 13:00 on the 18th June 2023. A concern was identified relating to the access PC Matthew Gell had made to the nominal record of Valdo Calocane and to occurrences linked to him without a clear policing purpose. PC Matthew Gell was a Response officer based at Radford Road Police Station at the time and he had accessed the NICHE subject record of Valdo Calocane on the 15th June 2023.
92. On the 18th June 2023 PC Gell was declared a subject of interest for Operation Glint and on the 19th June 2023, declared a criminal suspect for an offence of Misconduct in a Public Office.
93. PC Gell was arrested by Nottinghamshire Police on the 19th June 2023 and his personal mobile phone was seized. PC Gell was interviewed under caution, released from custody on police bail and suspended from duty. A mandatory referral of his conduct was submitted to the IOPC under reference CM/49/23. I

[1] Criminal and Justice and Courts Act 2015

refer to this as police item NGPF0007871 . This was due to PC Gell meeting the criteria that there was an indication of a serious criminal offence (those which carry a fixed sentence or a minimum sentence of seven years), namely Misconduct in a Public Office. The IOPC subsequently determined the matter would be locally investigated by Nottinghamshire Police under paragraph 16 of Schedule 3 of the Police Reform Act 2002.

94. Between 20th and 23rd June 2023, the personal mobile phone of PC Gell was examined. This revealed that he sent a message to an associate, Matthew Hopewell who did not work in policing, indicating that the incident had been declared internally as a terrorist attack. Although not the case, had it been true it was clearly sensitive operational information which should not have been shared.

95. In addition, the following message was discovered to have been forwarded by PC Gell to his wife who is not a police employee and an officer (PC Ricky Brookes) serving with West Midlands Police:

"So 2 students on ilkeston Road have been proper butchered, 4 section turned up and tried to hold their inners in. Suspects then made off and attacked a man in a car on magdala and stabbed him to death, He's then made off towards town and ran over 4 other people who are in hospital now. He's then made his way back to radford and been stopped and tasered on spot. He's refused his details pulled his prints at custody and he's wanted on Derbyshire and Leics He lives in Birmingham but also has an address in Mapley. There are 32 cops covering 5 scenes at the minute all on TG7 the whole of city not involved in [*sic*] on TG4. 4 section have just left with some going up to trim. Half aren't going to be working tonight so be prepared to be asked to stay on."

96. The reference to '4 section' relates to the Response team on duty at the time of the attacks. The terms 'TG7' and 'TG4' relate to the airwave channels these geographical areas would be covered by. Talk group 7 included the area of Radford Road. Talk group 4 covered an area outside of the City with the interpretation being that the radio traffic on Talk group 7 was so busy that anyone else dealing with any other incident was moved to a different geographical Talk group. TRiM refers to Trauma Risk Management. This is a structured, peer-delivered support system designed to help officers and staff cope with the psychological impact of traumatic incidents. It is my personal opinion that the author of this message was actually referring to the Post Incident Management procedure ("PIM") rather than TRiM.

97. The WhatsApp message which was sent to PC Gell (which he subsequently forwarded on to his wife and PC Brookes) was not captured on the mobile phone of PC Gell because the 'disappearing messages' feature was switched on. It could only be viewed because he had forwarded the message to his wife and an officer from another police force. During a formal interview on the 20th July 2023, PC Gell confirmed that the person who sent the WhatsApp message to the group was PC Ashley Small. PC Small was, and still is, a Response officer in Nottinghamshire Police.

98. I have not found documentation which provides a list of those in the WhatsApp group called 'The Section' to which the message was sent. However, the mobile phone evidence from PC Gell showed commentary between him and two other colleagues which indicated that they were all receiving messages in the group called 'The Section.' One of these colleagues was PC Eliot Meynell, a Nottinghamshire police officer and the son of Chief Constable Kate Meynell.

99. The CCU SIO Digital Policy Document for Op Glint NGPF0005635 completed by DI Harding recorded the following decision at 15.02 hours on the 23rd June 2023: "The message does not contain information that is particularly sensitive but does contain emotive/graphic description of events. In relation to PC Small at the present time it would appear he has simply sent the original message to a shift WhatsApp group or to colleagues. We have no evidence he has disseminated the information wider than this at present. At the present time I do not see that this would constitute misconduct or a criminal act. I have therefore made the decision that an appropriate and proportionate course of action will be to speak with PC Small to establish the facts around the message i.e. who he sent it to, his motivation in sending it and whether he passed the message to persons outside the organisation. I also intend to ask that he shows us the messages he did send but do this acknowledging that we have no legal basis to demand his device other than if PC Small was to voluntarily provide it to us."

100. On the 23rd June 2023, an Ethical Interview and Intervention took place with PC Small in the presence of his Inspector NGPF0005569 Ethical Interviews and Interventions are not set out in policy or legislation. They are used by PSD to challenge inappropriate behaviour to ensure that the individual is aware that they have (or may have) breached the Standards of Professional Behaviour and to ensure that they learn from feedback and are hopefully thereby prevented from repeating the behaviour. The document of the intervention is retained on their Centurion record.

101. PC Small was not under the misconduct caution nor was he served a notice of investigation under the Conduct Regulations. PC Small confirmed that he sent the message with a purpose to pre warn the team about what they

would be coming onto. He reflected that the language was insensitive and may not be considered professional. It is recorded in the document that he was very apologetic and humble. The record of the intervention does not list those who were in the group. PC Small stated that it was his Response shift and did not include the Sergeant.

102. It is my opinion that the content of the WhatsApp message was both insensitive and unprofessional. It lacked empathy for the victims and their families, but also for his colleagues who had attended the scenes on the morning of 13/06/2023. However, it was sent by PC Small, to their police colleagues only, to warn them of the probability of an extended shift. It is recognised that police officers are exposed to more traumatic incidents that the average person and as a result can become emotionally desensitised as a coping mechanism. I agree with DI Harding that this was not a breach of the standards of professional behaviour that was so serious as to justify disciplinary action.

103. The action of PC Small was distinct from the actions of PC Gell who had accessed information without a policing purpose and had shared operational information with persons outside of policing.

104. Although PC Gell had been identified from Lawful Business Monitoring, the researchers in PSD continued to review systems access with the objective of identifying anyone who could have unlawfully provided information to the media. For this reason, PSD's focus was on people accessing the NICHE nominal record for Valdo Calocane.

105. The SIO Digital Policy Document for Op Glint records that on the 4th July 2023 DI Harding reviewed the evidence in relation to PC Gell and made the

decision that he should be 'refused charge' for the criminal offence. There was no evidence that PC Gell had provided information directly or indirectly to the media. PC Gell had viewed crime and intelligence information relating to Calocane but had not accessed the records relating to the attacks of the 13th June 2023. PC Gell had not viewed or accessed any other material relating to the Op Hendrix investigation.

106. DI Harding noted: "In this case I don't see that Gell has misconducted himself in a way that abused the public trust. I also do not feel that the misconduct "injures the public interest" either and feel that the actions of Gell do not meet the threshold to be considered criminal. I am therefore satisfied that the investigation should move from the criminal to misconduct arena and proceed under those regulations."

107. The investigator, DC Lee Keeling, finalised his misconduct investigation on the 8th September 2023 and the then Head of PSD and Appropriate Authority (D/Supt Williams) made a determination that PC Gell had a case to answer for gross misconduct on the 14th September 2023. The allegations were that he had shared operational information with his wife, PC Brookes and Matthew Hopewell without lawful authority or reasonable excuse and that he had accessed and searched Niche systems in relation to Valdo Calocane without a policing purpose.

108. PC Gell appeared before a Misconduct Panel on the 19th January 2024 and was found to have committed Gross Misconduct. He received a 2-year Final Written Warning. The independent Legally Qualified Chair for the panel was Mr Oliver Thorne of counsel.

109. The PC Gell hearing was conducted in public, the officer was named and media were present.

110. A final written warning under the Police (Conduct) Regulations 2020 is a formal disciplinary sanction issued to a police officer when their conduct is found to amount to misconduct or gross misconduct. It is one of the possible outcomes of misconduct proceedings and is more serious than a written warning but less severe than dismissal. A final written warning typically remains in force for two years from the date it is issued, though in exceptional circumstances, it can be extended up to a maximum of five years. It serves as a clear notice that any further misconduct during this period could lead to more severe disciplinary action, including dismissal.

Audit of Systems

111. DI Harding produced a document titled 'Op Hendrix – PSD investigation overview.' I refer to this as police item NGPF0007874 . He described the work undertaken to identify any individual who may be leaking information to the media. He stated: "The Counter Corruption Unit carried out police system audit activity covering the period 13/06/2023 to the 16/06/2023 around persons who had accessed the nominal record of CALOCANE on Niche. The record had been opened 381 times by 179 members of Nottinghamshire Police. Due to the volume of members of Nottinghamshire Police viewing the records; a decision was made that Officers / Staff in roles such as Major Crime, EMSOU Forensic Services and CID teams would be excluded from further follow up work due to the likelihood of operational involvement (scene /investigation/post event work). Where their respective activity could not readily be seen to be legitimate from

research; individuals were sent emails (copied into their Line Managers) asking them to account for their actions (with exception of a member of Police Staff who was subject of a Severity Assessment and a Criminal / Gross Misconduct investigation commenced). In addition, a number of self-referrals were also received by the Counter Corruption Unit and investigated. Following this process 22 people were identified as causing the most concern.

- 10 were found to have had legitimate access to the records and had a policing purpose to do so.
- 4 were referred to local line management and were given advice regarding accessing records.
- 3 were found to be partnership workers and an intervention was conducted with each in the presence of a senior manager from that agency and a note added to their vetting file.
- 2 had an intervention with Counter Corruption officers and were issued with a negative performance record.
- Of the remaining three these individuals have either been through or are pending a misconduct process."

112. The 4 persons referred to local line management had all accessed the SAFE Command and Control incident log and NICHE record for Calocane. They were all found to have been self-briefing as they were informed that they were required for scene preservation. They had not accessed any other material relating to the investigation. I have been unable to identify the documented justification for this decision but would hypothesise that it was

decided that whilst they accessed the material for a policing purpose, the extent to which they did so was not justified.

113. This reiterates my point that line managers must set clear parameters when individuals are directed to 'self-brief' so that there is no ambiguity about what material can be viewed and for this reason they received words of advice from their line manager.

114. The 3 partnership workers (Community Protection Officers) from Nottingham City Council who had interventions with CCU and a senior line manager, had accessed NICHE information relating to Valdo Calocane as well as the crimes created as occurrences on the 13th June 2023. One of them accessed the forensic report for victim Barnaby Webber. PSD were not satisfied that they had a policing purpose for accessing the data and as part of the intervention they were informed that there would be a note on their vetting file. Nottinghamshire Police was not responsible for any misconduct matters in respect of these Community Protection Officers as they are not employed by the police. A Community Protection manager was present during their intervention.

115. For the two individuals who were the subject of an intervention by CCU and issued with a negative performance record, PC Emily Dunn had entered the Safe incident logs and Niche records for Operation Hendrix and furthermore entered Officer Enquiry Logs (these provide investigative updates), the case file (this is where documents are collated in anticipation for sharing with the CPS) and sudden death report for Grace O'Malley-Kumar. She was given an intervention on 20th July 2023 and a negative performance record. This ensured

that there is a formal record of the intervention on her personnel file for corporate memory.

116. The second individual was a member of police staff, Christopher Wiles, who approached his line manager following the whole force email dated 22nd June 2023 sent out reminding employees of their obligations. He reported that he had checked the occurrence or person on two occasions whilst he was on annual leave. He had no policing purpose for doing so. He was given an intervention on the 24th July 2023.

117. The SIO Digital Policy Document has an entry dated 4th July 2023 recording that DI Harding reviewed the audit data produced by the CCU researchers and made the decision that 2 police officers and 1 member of staff would be subject of further scrutiny. This was due to the number of checks completed by them, the time of the checks and the content viewed.

118. One of the police officers was PC Emily Dunn (who subsequently received an intervention), the second was PC Agata Lasek who had viewed the SAFE incident and NICHE records for Valdo Calocane. It was established that PC Lasek was self-briefing because she was deployed to the scene but had viewed additional material believing that she had previous and recent contact with Valdo Calocane. It was accepted that PC Lasek's access of police systems was for a policing purpose.

Sarah Rutherford

119. The member of staff subject to additional scrutiny was front counter staff member Sarah Rutherford and further audit work was conducted by CCU.

120. The SIO Digital Policy Document has an entry dated 12th July 2023 stating: "On further review of material in relation to police staff member Sarah

Rutherford I have decided that this enquiry should move into the criminal arena".

121. On the 13th July 2023, an IOPC referral regarding Sarah Rutherford was submitted on the basis that there was an indication of computer misuse. This was submitted under Centurion reference CM/57/23. I refer to this as NGPF0007872. The IOPC determined that this should be investigated locally by Nottinghamshire Police.

122. On the 14th July 2023 Sarah Rutherford was arrested for the following offences:-

a. Cause a computer to enable unauthorised access to a program/data - Contrary to section 1(1) and (3) of the Computer Misuse Act 1990.

b. Knowingly / recklessly obtain or disclose personal data without consent of controller - Contrary to section 170(1)(a) and 196(2) of the Data Protection Act 2018.

c. Conspiracy to commit misconduct in public office - Contrary to section 1(1) of the Criminal Law Act 1977.

123. Following interview on the 14th July2023 Sarah Rutherford was released under investigation and suspended from duty.

124. On the 29th August 2023 Sarah Rutherford was given an adult caution for the offence of "causing a computer to perform a function to secure or enable unauthorised access" under Section 1 of the Computer Misuse Act 1990. This was following admissions during interview about accessing numerous cases without a policing purpose.

125. Running alongside the criminal investigation into Sarah Rutherford was the misconduct investigation and on the 28th November 2023 the misconduct

investigator finalised his investigation report. He concluded that in relation to the events of 13th June 2023, Sarah Rutherford had searched NICHE for the subject Valdo Calocane and accessed his record as well as records relating to a Nottingham address Calocane was showing as linked to. Rutherford had also accessed a NICHE nominal record GRO-E She viewed SAFE Command and Control incidents relating to the events of 13th June 2023 and conducted intelligence searches for the subject Valdo Calocane. She did not view any CCTV or Body Worn Video evidence.

126. Rutherford also extensively viewed other material unrelated to this inquiry which she was not entitled to and on the 7th July 2022 had been given a warning by CCU about the importance of only accessing material for a policing purpose.

127. A Police Staff Misconduct Hearing into Rutherford took place on the 5th April 2024 and found the allegation proven to the level of gross misconduct and determined that Rutherford would be dismissed with immediate effect. She has been placed on the Barred List. Because police staff are not public office holders, their disciplinary hearings are treated as internal employment matters, and the ACAS Code dictates that their hearings are conducted in private.

Special Constable Skenderaj

128. On the 1st September 2023 SC Skenderaj sent an email to Det Supt Williams disclosing that on the 31st August 2023 he viewed Body Worn Video (BWV) footage that was captured in relation to the Valdo Calocane investigation. Research showed SC Skenderaj had 'downplayed' the extent to which he had accessed sensitive footage relating to the murder victims. He had

also conducted research on policing systems of himself and other nominals with no apparent policing purpose.

129. SC Skenderaj disclosed that he had viewed the footage at his home address whilst off duty and admitted that he had no policing purpose. He described his actions as stupid, foolish, inconsiderate and morally wrong.

130. The recordings SC Skenderaj viewed included the arrest of Calocane, officers and paramedics providing medical assistance to the victims Barnaby Webber and Grace O'Malley-Kumar, footage within an ambulance, and both victims being placed in body bags.

131. SC Skenderaj also accessed the NICHE record of Valdo Calocane and from that opened the occurrences he was linked to relating to the attempted murder of Sharon Miller and Wayne Birkett, the assault on a detention officer and an intelligence report for Valdo Calocane.

132. SC Skenderaj was informed that he was under investigation on the 8th September 2023 and suspended from duty. On the 13th September 2023 he resigned from Nottinghamshire Police.

133. The investigator nonetheless continued with the investigation and on the 3rd October 2023 reached a decision that they believed the Special Conditions for an Accelerated Misconduct Hearing (i.e. fast track) were met. Under the Police (Conduct) Regulations 2020 proceedings can continue in certain circumstances against former officers.

134. On the 12th October 2023 DCC Cooper determined that the special conditions were met and that the matter should be referred to an Accelerated Hearing for which the chair is the Chief Constable.

135. Chief Constable Meynell made the decision that the matter would be held in private. In her Regulation 53 (of the Police (Conduct) Regulations 2020) 'Public notification of accelerated misconduct hearing notice' decision she stated the following:

"The Home office Guidance provides examples at 11.84 of relevant factors that may be taken into account in considering whether to hold a hearing in public or private. There is an overriding presumption that hearings should proceed in public. However I have considered the submission from the Federation and the impact a public hearing would have on those individuals who are victims of SC Sjenderaj (sic) alleged misconduct. There is also an ongoing criminal investigation and it is paramount this is not jeopardised. This is in addition to an ongoing Coroner's Inquest. As such the hearing (sic) my decision is that the hearing should be held in private."

136. On the 11th December 2023 Chief Constable Meynell chaired the Accelerated Misconduct Hearing and found (under the Former Officer provisions) that SC Skenderaj would have been dismissed without notice had he still been serving. He was therefore placed on the Barred List and the necessary documentation was sent to the College of Policing.

137. There was no audit undertaken by CCU to establish whether anyone had viewed BWV or CCTV footage without a policing purpose. I have been unable to identify any policy decision in relation to this. It appears clear that concern raised within force was that information was being leaked to the media and that such leakage would undermine the investigation. Therefore, the then Head of PSD, D/Supt Williams, provided DI Harding with the objective to identify any person with access to Nottinghamshire Police systems who could be

responsible for a leak of information. For this reason, Operation Glint focused on the record of Calocane because it was in relation to information about him being in the public domain which had resulted in the concern.

Steps which could or should have been taken to protect the integrity of the sensitive data, information or material and the dignity and privacy of victims and survivors, including the bereaved families

138. Discussions relating to the possibility of restricting access to information took place in Gold group meetings on the 14th June 2023 and 20th June 2023. The decision was made by ACC Griffin not to restrict access.

139. I believe the decision by ACC Griffin was taken from the perspective of conducting an efficient criminal investigation into Calocane's actions and ensuring that all those officers and staff who were able to contribute evidence and information were able to do so efficiently as well as ensuring those investigating very serious crimes could readily access the information that they required.

140. The dignity and privacy of victims and survivors is protected by the requirement that officers and staff will obey the rules in relation to access and sharing and not misconduct themselves by looking at or sharing material for which they have no legitimate purpose to access.

141. The position taken by Nottinghamshire Police was not to eliminate any possibility of someone being able to misconduct themselves by accessing material without a policing purpose. Instead, it was to invest energy and effort into reminding people of their legal obligations and taking enforcement action against those who breach these obligations.

142. The reminders are there every time personnel log onto a system, through training (initial and ongoing) and through the annual Integrity Health Check. In addition, I believe that those who have misconducted themselves in this manner have been publicised on the intranet as a further reminder and warning to others.

143. I believe it would be challenging to articulate and then enforce a policy to inform decisions about when to restrict information across all systems and what information to restrict. Nottinghamshire Police receives and records data, information and material of a sensitive nature on multiple occasions every single day.

144. There are 12 nationally agreed corruption categories used in UK policing. These categories are defined by the National Police Chiefs' Council Anti-Corruption Advisory Group (NPCCAG). These categories are primarily used by CCU's to record and analyse intelligence related to corruption threats within police forces.

145. The "Computer Misuse" corruption category in UK policing refers to the unauthorised or inappropriate use of police computer systems, and it is governed primarily by the Computer Misuse Act 1990.

146. There is a separate corruption category to cover 'Disclosure of Information.' This relates to the unlawful disclosure of information to a variety of sources from family and friends through to the media and criminal groups and thus has the potential to compromise investigations.

147. In hindsight, I believe that the objective provided to the CCU SIO, to focus on the concern that information was being shared outside of policing, was the correct priority. However, I do reflect that, capacity permitting this should

have extended into researching who had accessed sensitive information without a policing purpose, and that anyone found doing so should have been subject to a misconduct investigation. I believe therefore that this should have extended into areas beyond just the record of Calocane and specifically to the BWV footage. If there was insufficient capacity, then this should have been documented to provide context.

148. I believe the interventions for police employees who viewed material without a policing purpose were inadequate, as the message to hold them accountable was not effectively enforced.

149. This is learning which has been taken by PSD because of and in advance of this public inquiry. In particular, in respect of the question as to who would have a legitimate purpose to view BWV and CCTV which arguably impacts most significantly on the dignity and privacy of victims, families and survivors.

150. On reflection, I believe the message sent to all Nottinghamshire Police email accounts on the 22nd June 2023 was unclear and lacked sufficient impact. I believe that this should have been communicated by a member of the Chief Officer Team (Chief Constable, Deputy Chief Constable, Assistant Chief Constables). The message states that if personnel have accessed material they will be held to account but advises them to tell their line manager, or the staff association or PSD. I do not believe that material was provided to line managers to explain what was expected of them following such a disclosure, for example, an expectation that they notify PSD for an assessment to be made.

151. In conclusion, whilst it was possible to restrict access to information and this step 'could' have been taken, I do not believe that this is a step which

'should' have been taken. I do not believe that it is possible to eliminate the risk of an employee misconducting themselves by restricting access to material without impacting on the ability of officers and staff to deliver a service to the public.

Steps taken to ensure that the survivors and bereaved families were appropriately informed concerning any data breaches and the actions taken

152. On the 20th September 2023, an email chain was started by Detective Inspector (at that time) Claire Gould. DI Gould was the Family Liaison Co-ordinator (FLC). I refer to this email chain as NGPF0007867 . This was sent to Family Liaison Officers DC McVey, DC Farrell and DS Kimberley. I would summarise this as a message informing them that PC Matthew Gell was facing a Gross Misconduct Hearing for misuse of police systems and disclosing information and that the families need to be made aware of this. She commented that it was important to be open and honest. She explained that PC Gell had shared a WhatsApp message with persons outside of policing and that she did not intend to share the content of the WhatsApp message. She explained that she was waiting for D/Supt Williams to confirm that this could be shared.

153. D/Supt Williams responded on the same date (20th September 2023) and copied in several other people; ACC Griffin, DCC Cooper, DI Harding, DCI Reynolds and Stephen O'Connell (the PSD hearings and meetings officer). She confirmed that other than releasing the officer's name (because at that time it had not been confirmed by a chair whether the hearing would be in public or private or anonymised), that she was content with the proposal and wording.

She clarified that if the hearing was held in private the families could potentially attend, with the agreement of the chair and that potentially they could provide a statement about the impact. She also informed those in the conversation that there was a Special Constable who had admitted viewing a lot of the most distressing footage. She confirmed that he was suspended and anticipated that he would proceed to an Accelerated Misconduct Hearing.

154. ACC Griffin responded on the 20th September 2023 and in summary confirmed that he was keen for the family to find out about these misconduct matters.

155. On the 6th October 2023, an email was sent by DI Claire Gould to DC McVey, DS Kimberley, DC Farrell, DC Piggott, PC Baxter and copying in DC Cutts. There is no subject header. I refer to this as NGPF0007868 . This provided a summary of the 3 PSD investigations; PC Gell, PC Skenderaj and Sarah Rutherford. DI Gould stated that she was awaiting a form of words from D/Supt Williams to ensure the information was correct before sharing with the families the following week. She commented that it was crucial that they were upfront about this and wanted to ensure that they received things as timely as possible.

156. An SIO policy log entry completed by D/Supt Sanders and dated 13th October 2023 contained the following: "Professional Standards and information access: At this moment in time and until I get any further direction and information as SIO, there will be no dialogue with families surrounding PSD matters, as we simply have not had clarity as to the situation. In all good conscious (sic), I am not aware of any press leaks by employees as previously thought (and rumoured) if officers have looked at material without a policing

purpose, to date that is only an allegation, will have to undergo due process and then we will be informed. Until formal notification to the contrary, there is simply nothing further to add or update families about."

157. On the 24th November 2023, the SIO D/Supt Sanders made an entry in his SIO log stating: "informed at the Gold Group that there were no PSD matters that require further attention. PSD are of the belief that there are no further PSD /IOPC issues that are in need of addressing. IE all matters are closed and there appear to be no issues."

158. On the 8th December 2023 D/Supt Sanders noted in the SIO log that he intended to meet with the family of Ian Coates. He commented that amongst other updates regarding the investigation he would update on misconduct issues.

159. On the 12th December 2023 D/Supt Sanders emailed T/Supt Reynolds requesting a list of all PSD investigations, details of dates of investigation and outcomes. I refer to this email as NGPF0007884 . D/Supt Sanders commented that the families would ask why they have not been informed of any PSD investigations to date. D/Supt Sanders stated that he may require PSD to update the families and does not wish to drip-feed PSD matters. He wished to meet with T/Supt Reynolds to discuss the detail.

160. T/Supt Reynolds responded within the email chain to state that he believed that the investigation team had been previously briefed on the investigations. He noted that at the Accelerated Misconduct Hearing (AMH) for former SPC Skenderaj, chaired by Chief Constable Kate Meynell the previous day, she had directed that the family be informed.

161. On the 14th December 2023 D/Supt Sanders sent an email to ACC Griffin copying in T/Supt Reynolds and DI Gould. I will refer to this as URN NGPF0007883. D/Supt Sanders pointed out a number of issues which included the requirement for families to be provided with full details of the cases which were not known and any safeguards the organisation had put in place to prevent it happening again. D/Supt Sanders sought guidance from ACC Griffin.

162. ACC Griffin responded on the same date. He stated that he believed that some information had already been disclosed relating to the PSD investigations and he acknowledged that one employee had viewed images of the deceased. He stated that an immediate duty of candour was triggered. He directed that the family of that person should be informed immediately, by which he elaborated "in the next few days."

163. On the 18th December 2023, D/Supt Sanders documented in his log that he had met with the Head of PSD and noted: "FLO's to be appraised of PSD matters so that if required can provide briefing to families. I have been informed of the ACH (*sic*) regarding SPC Skenderage *(sic*) and his dismissal for accessing police information without a policing purpose. This includes material around Operation Hendrix in addition to other checks he had undertaken. There is no suggestion that he has passed any material to a third party. A form of words to be agreed by SIO and PSD lead and GOLD before dissemination to families. It will also have to be delivered at a time when they can digest and understand the decision. This is preferable either in a TEAMS meeting or face to face."

164. I am aware from the FLO log of DC McVey that on the 15th December 2023 a meeting was held between the SIO, the then Head of PSD (T/Supt

Reynolds), and some of the Family Liaison Officers. T/Supt Reynolds provided a verbal update on the SPC Skenderaj investigation and updated that there were 2 further matters pending (Gell and Rutherford) where material had been accessed without a policing purpose. It is noted that there was a discussion about whether it was appropriate to share the information with the families that week on top of their distress over the discussions relating to diminished responsibility and manslaughter. A decision was made by the SIO dated 15th December 2023 that disclosure of PSD matters at that time was not appropriate and that he would liaise with the Chief Officer Team.

165. On the 18th December 2023, the SIO log has an entry detailing a decision to meet with the family of Grace O'Malley-Kumar on the 19th December 2023 and to provide updates, to include PSD issues. However, a subsequent update notes that this meeting would not take place in person and that the meeting would take place on TEAMS with the Webber family instead.

166. On the 15th January 2024, the SIO log has an entry that a TEAMS meeting had taken place and that whilst this predominantly focused on the matters relating to the criminal trial that the Webber and O'Malley-Kumar families were updated that SPC Skenderaj had been dismissed for accessing case material.

167. On the 20th February 2024 Chief Constable Kate Meynell wrote to all families and set out the detail of each PSD investigation and outcome. Within her correspondence she apologised that they had not been kept updated and stated that there had been no intention of keeping the matters hidden from them.

168. I exhibit a copy of the letter as URN NGPF0007857, NGPF0007858, NGPF0007859.

Improvements which could or should be made to the process for communication with victims and families in such circumstances

169. In my opinion, the process for communicating with victims and families was appropriate: PSD shared investigation updates with the Gold group to keep the SIO and FLC informed. If this was not possible, information was given directly to the FLC and SIO. The SIO is responsible for all decisions relating to updating families and victims. PSD should not provide updates directly, as this could confuse or upset families who expect contact through their FLO.

170. However, I do believe that there was a duty of candour in providing updates as soon as possible and indeed this was referenced by Chief Constable Meynell and ACC Griffin. I believe that the SIO and PSD could have worked more closely together to ensure that the families were provided with information in a way which would not have compromised any misconduct proceedings.

171. The Police (Conduct) Regulations 2020 define an 'interested person' as "a person who has an interest in being kept properly informed about the handling of a complaint or conduct matter in accordance with section 21 of the Police Reform Act 2002"

172. In hindsight, this status and the duty that this brings, including keeping 'interested persons' updated, would have provided clarity and focus on the

expectations of the police to update the victims and families. This would have included updating the families of the public hearing of PC Gell.

Protocols which govern the management of video footage and evidence in the investigation and prosecution of high-profile cases

173. In the UK, the management of video footage and evidence in high-profile police investigations is governed by a combination of statutory codes, national guidance, and operational protocols.

174. The Forensic Science Regulator's Code of Practice (FSR COP) sets out mandatory quality standards for the capture, retrieval, processing, and storage of digital evidence, including CCTV and video surveillance systems (VSS). It ensures that evidence is admissible in court and maintains integrity and continuity throughout the investigative process

175. The National Police Chiefs' Council (NPCC) Framework has developed a Digital Evidence Management (DEM) standard, which outlines how forces should manage digital evidence, including: Chain of custody, Metadata preservation, Secure storage and access controls.

176. The NPCC Framework for Video-Based Evidence (NPCC FFVBE) is a formal, structured approach developed to ensure the lawful, consistent, and forensically sound handling of video evidence across UK policing. It is enforced under the Forensic Science Regulator Act 2021 and aligns with statutory codes and national standards.

177. College of Policing Guidance CCTV Authorised Professional Practice offers operational advice on CCTV recovery, including:

a) Scene assessment

b) Technical compatibility

c) Ensuring footage is not overwritten or degraded.

178. I have caused the Major Crime Investigation Manual (MCIM) and the Major Incident Room Standardised Administrative Procedures (MIRSAP) documents to be reviewed.

179. These are wide ranging documents that provide national best practice for management of evidence / material in major crime investigations.

180. Their focus is on how evidence is processed through a Major Crime room – the way it moves between the different roles (receiver to indexer to typist to proof-readers to office manager and on finally to disclosure officer). What this means in plain English is a very rigid system in which things are read (or in the case of video-footage, where the written notes made about it are read) multiple times to make sure nothing is missed or overlooked.

181. MCIM provides the strategic and investigative framework. MIRSAP delivers the administrative and procedural backbone to support that strategy. Together, they ensure that major investigations are thorough, accountable, and consistent, regardless of jurisdiction.

182. Nottinghamshire Police have procedure PD 510 'CCTV (Closed Circuit Television) Material. Procedure for Recovery, Viewing and Presentation.' I produce this as NGPF0007416 This has a registered owner of the Head of Crime and Author is the Digital Capabilities Lead.

183. This procedure states that it will assist in compliance with both the FSR COP and the NPCC FFVBE.

184. The aims and objectives of this procedure are set out as:

a) To highlight the importance of professional and accurate CCTV enquiries.

b) To identify key roles and responsibilities to ensure the best advantage is made of this material.

c) To provide uniformity in the processes of recovery, viewing and presentation of CCTV material.

d) To signpost form G866, which ensures consistency and uniformity in the recovery of CCTV

e) Outline training levels and requirements to complete CCTV related work.

f) To ensure that all CCTV evidence is presented lawfully and professionally in court proceedings

185. Because I am not a subject matter expert in relation to this area, I have sought expert opinion from Detective Inspector Mark Booth who is the author of the procedure PD 510. He has oversight of the Digital Multimedia Evidence Unit, which is responsible for the forensic acquisition and analysis of audio-visual material and has been in that role for 3 years. DI Booth has worked in the field of digital forensics and cybercrime investigation for around 10 years. He has an MSc in Cybercrime Investigation, and several industry qualifications in digital forensics. As a result of information received from him I can state the following.

186. I would be inclined to define the "management of video footage and evidence" in the following terms:

a) Acquisition (or retrieval) – the recovery of relevant material from the source into a police system.

b) Processing – the movement of relevant material between police systems, and the conversion of it from one format to another. Also includes the

compilation of footage for presentation purposes. In some cases, will include expert analysis too, for example, assess authenticity.

c) Presentation – the processing of evidential material from police systems to the CPS and partner agencies.

d) Storage – the holding of any material at rest in a police system, including the appropriate disposal.

187. Policy PD510 'CCTV (Closed Circuit Television) Material. Procedure for Recovery, Viewing and Presentation' was written with the assistance of an expert team. The intention of that document was to professionalise and standardise the first three parts of the above list. It does not consider storage, which is a logistical issue rather than a forensic science activity.

188. The storage of recovered digital material in Nottinghamshire Police takes place in the Digital Evidence Management System, which is called NICE Investigate. NICE investigate is a third-party system that is supplied to Nottinghamshire Police under contract, to meet the conditions stipulated in the NPCC Digital Evidence Management (DEM) standard. NICE is used in several UK police forces and other agencies. In addition to storage, NICE also offers automation of some aspects of acquisition, processing, and presentation. Audio-visual material is key evidence in almost every modern investigation, meaning that NICE investigate handles a vast quantity of data and needs to be accessed by a variety of people during the lifespan of an investigation.

189. NICE is fully audited, to provide full chain of custody for every evidence item. When an authorised user opens NICE, they are faced with a declaration that they must interact with to proceed.

190. Most of the functions of NICE are concerned with preserving the forensic reliability of the evidence that it contains. File integrity is checked with file signatures, and a chain of custody is maintained every time a file is accessed.

191. A file can be uploaded to NICE by an internal user, an external provider via upload link, or an automatic connecter from another internal system, such as body worn video.

192. After upload, files are automatically archived after 30 days. After archive, the file must be retrieved by anyone needing to access it. This is an interactive process requiring the user to select the option to retrieve the file before viewing it. The process can take up to 24 hours.

193. It is possible to restrict access to a case within NICE. Access to material is governed by the original officer in the case and is granted on an individual basis. Once restricted, the entire case is locked to all until permission is granted. When a case is restricted in NICE, users without permission are still able to upload to the case, but they cannot see the contents. Permissions are granted to the entire case, not individual items within it. Access restriction is not commonly used due to the often large number of people inside the police who require access to material, including those outside the investigation team, such as intelligence teams and specialists in forensic units.

194. The forensic science regulator's codes of practice are also largely concerned with forensic reliability of evidence that is handled in a forensic science context. Storage is referred to generally in section 23. 23.1.2 dictates that storage should be sufficient to prevent loss, deterioration, and contamination. 23.1.3 states that access to storage (and server rooms) should be restricted to authorised personnel. Section 26 of the code considers the

security of electronic information. 26.4 is titled "Access control to electronic information." It sets out controls that should be in place to restrict access to information to those within a forensic unit. It does not consider the storage of data outside of a forensic laboratory system, and the terms of the code should not be applied beyond that scope.

195. Having considered this question, it appears that all the policies and protocols that have been developed in UK policing concerning the management of digital evidence are centred on maintaining the forensic integrity and reliability of that evidence. Very little consideration has been given to preserving the dignity, and/or the privacy of those who are the subjects of that evidence. Some aspect of almost every crime are captured in audio-visual material, including often graphic detail of rapes, murders, road deaths, industrial accidents, and child abuse. That evidence is often critical to understanding the unadulterated truth.

196. The focus will always be on enabling efficient gathering, storage and access to video evidence in all cases.

197. Policy PS 163 Acceptable Use Policy and Generic Security Operating Policy (SyOps) for all Police Information Systems (NGPF0007438) sets out the expectations of Nottinghamshire Police for those accessing <u>any</u> policing system. The principle of accessing only for a policing purpose are relevant to video footage captured in the investigation of high-profile cases and I believe that the existing codes and warnings should be sufficient.

<u>Matters to bring to the attention of the Chair</u>

198. Restrictions were only put in place on one force system, the Command and Control system, SAFE, where the incident log was restricted in line with the policy to restrict following a Post Incident Procedure.

199. It would have been possible to restrict the occurrences in Niche though in my opinion that would have significantly hindered the investigation or would have required a team of people dedicated to giving access to individuals as and when required.

200. I believe that restricting one or more of the occurrences would have created significant logistical challenges for Nottinghamshire Police and in tenson with the objective of effectively and expeditiously investigating the crimes to reach a successful charge within the time constraints of Police and Criminal Evidence Act 1984.

201. The NICE Investigate system does not allow individual exhibits to be restricted; it will only allow the entire master record to be restricted. Due to the volume of people working on the investigation this would have been logistically challenging with individuals having to request access to the record. It was essential to store all digital exhibits in one location to enable the Major Crime enquiry team to access and review the relevant material.

202. The position taken by Nottinghamshire Police was not to eliminate any possibility of someone being able to misconduct themselves by accessing material without a policing purpose. Instead, it was to invest energy and effort into reminding people of their legal obligations and taking enforcement action against those who breach these obligations.

203. This decision was made by ACC Griffin during a Gold group on 14th June 2023 and the direction not to view material without a policing purpose was

cascaded through the commands. There was an email sent to every person in Nottinghamshire Police to reinforce this message.

204. The reminders are there every time personnel log onto a system, through training (initial and ongoing) and through the annual Integrity Health Check. In addition, I believe that those who have misconducted themselves in this manner have been publicised on the intranet as a further reminder and warning to others.

205. I believe it would be challenging to articulate and then enforce a policy to inform decisions about when to restrict information and what information to restrict. Nottinghamshire Police receives and records data, information and material of a sensitive nature on multiple occasions every single day.

206. Nottinghamshire Police employees are clearly informed during both initial and ongoing training, as well as warning notices on individual systems, that accessing material without a policing purpose is strictly prohibited. We are committed to reinforcing this message through continued in-person training and by ensuring consistent communication on this subject.

207. The introduction of the Annual Integrity Vetting Review (AIVR) in January 2025 as a result of the updated Vetting Authorised Professional Practice (2025), further reinforces this message. The Vetting APP details a requirement that every member of the police service completes an AIVR with their line manager. It places a requirement on the line manager to ensure their staff are aware of, and adhere to Policies, procedures and guidance which exist to safeguard the public, officers, staff and the police service. This includes a section on 'Misuse of Force Systems and Disclosure of Information.'

208. The individual and their line manager must sign to say that they understand each policy, procedure or guidance and the expectations upon them. This is a more formal process, and as a result now replaces the Annual Integrity Health Check.

209. The Disclosure of Information outside of policing was a legitimate concern which threatened the integrity of the investigation, and I believe was appropriate as the primary focus for PSD resources. However, I do believe that following the initial audit there should have been consideration for additional audits of other systems, specifically BWV.

210. Furthermore, and on reflection, this inquiry has highlighted the requirement for supervisors to provide clear parameters to their team if directing them to 'self-brief.' Providing clear instruction about the specific material to be reviewed eliminates any ambiguity about whether such access serves a legitimate policing purpose.

211. I have introduced an expectation upon PSD that when attending Gold groups that we consider the following in our updates so that there is clarity for Gold, the SIO and FLC:

- IOPC referral requirements and progress updates
- any public complaints about the incident
- Assessment of the extent to which the Gold group objectives adequately address PSD-specific matters
- Consideration to provide a briefing on any proactive work being undertaken, and, if the information is sensitive, ensure that the Senior Investigating Officer (SIO) is appropriately informed.
- Conduct matters and updates as to progress

- Identification of interested persons associated with any DSI, recordable conduct, or complaint matters, and, if applicable, agreement on providing regular updates through FLO.

212. It is regrettable that a small number of officers and staff, entrusted with sensitive information and materials necessary for their duties, misused this trust by accessing material inappropriately. The actions of a few have detracted from the dedication and professionalism exhibited by the majority, including those initial responders who continue to be affected by the challenging circumstances they encountered.

Statement of Truth

I believe the content of this statement to be true. I understand that proceedings may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief of its truth.

Signed:

GRO-B

Dated: 05/12/2025

Index to First Witness Statement of KATHRYN CRANER

No.	URN	Document Description
1	NGPF0007438	The Acceptable Use Policy and Generic Security Operating Policy (SyOps) for all Police Information Systems (PS 163)
2	NGPF0007882	PSD Training Slide
3	NGPF0007451	Misconduct and Criminality Communications Policy (PS143)
4	NGPF0007442	PS 295 Restricted incidents and Authorised Access policy
5	NGPF0004863	Gold Group Meeting Minutes 14.6.23
6	NGPF0007863	DI Harding e-mail 09:53 14.6.23
7	NGPF0004635	Gold Group Meeting Minutes 20.6.23
8	NGPF0007866	E-mail to staff 22.6.23
9	NGPF0005638	CCU activity – Op Glint (subjects where formal action taken)
10	NGPF0007865	E-mail to PSD 09:22 14.6.23
11	NGPF0007865	E-mail L Bradford to PSD Various 14.6.23
12	NGPF0005639	Copy of Clue Reference 1557
13	NGPF0005854	Draft E-mail D/Supt Williams
14	NGPF0007871	IOPC Referral - PC Gell
15	NGPF0005635	CCU SIO Digital Policy Document for Op Glint

16	NGPF0005569	Notes of Ethical Interview – PC Small
17	NGPF0007874	Op Hendrix – PSD investigation overview
18	NGPF0007872	IOPC Referral – S Rutherford
19	NGPF0007867	E-mail chain – DI Gould to FLO 20.9.23
20	NGPF0007868	E-mail DI Gould to FLO 6.10.23
21	NGPF0007884	E-mail D/Supt Sanders to T/Supt Reynolds 12.12.23
22	NGPF0007883	E-mail D/Supt Sanders to ACC Griffin 14.12.23
23	NGPF0007857 NGPF0007858 NGPF0007859	Letter CC Meynell to Families 20.2.24
24	NGPF0007416	PD 510 'CCTV (Closed Circuit Television) Material. Procedure for Recovery, Viewing and Presentation'