Witness Name: Amy Holmes
Statement No: WITN0065029
Dated: 01 April 2026

THE NOTTINGHAM INQUIRY

SECOND WITNESS STATEMENT OF AMY HOLMES

I, AMY HOLMES, will say as follows: -

INTRODUCTION

1. I, Amy Holmes, Interim Chief Operating Officer for the Ministry of Justice ('MoJ') previously provided a witness statement to the Inquiry dated 2 August 2025 ('the First Statement') **[WITN0065001]**.

2. As I stated in paragraph 3 of the First Statement, I have been reliant on the work of various officials from across the MoJ and its Executive Agencies to provide my statement. I am due to give evidence before the Inquiry on 14 April 2026. In advance of giving evidence and in preparation for this date I have learned of some areas of the statement that require update, clarification and/or correction. I therefore provide this supplemental statement to assist the Inquiry for the purposes of:

   2.1. Correcting a matter set out in the First Statement;

   2.2. Clarifying certain issues that require additional explanation; and

   2.3. Updating the Inquiry on improvements or actions taken since the provision of the First Statement.

CORRECTION OF A MATTER IN THE FIRST STATEMENT

3. In paragraph 72 of the First Statement, I summarised the number of former His Majesty's Courts and Tribunal Service ('HMCTS') staff who had accessed information held within the Digital Case System ('DCS') when they were not authorised to do so. I was informed that there were three members of court staff in total, one from Lewes Crown Court and two from Nottingham Crown Court. In the course of preparing to give evidence it has been brought to my attention that there is an additional member of staff who was based at Nottingham Crown Court who accessed information held on DCS about Valdo Calocane's ('VC's') case on 21 September 2023, without a business need to do so.

4. I therefore wish to correct the information within paragraph 72 of the First Statement to draw the Inquiry's attention to this fourth member of court staff.

5. The fourth former member of staff was an Administration Officer employed by HMCTS as part of a Summer Intern Scheme, from 3 July 2023 to 25 September 2023.

6. The fourth former staff member's name was included in a report which detailed HMCTS staff who had accessed the VC case and was shared between HMCTS Counter Fraud Team and the HMCTS Operations Manager for Nottingham on 25 July 2024, to query whether access was authorised. On the same day, the HMCTS Operations Manager returned the list to HMCTS Counter Fraud with comments next to the fourth former staff member's name and the other former Nottingham members of staff outlined above, stating that they did not have business justification to access the case.

7. After this data gathering exercise, on 22 August 2024, HMCTS Counter Fraud Team took witness statements from HMCTS Operations and provided them to the police. These witness statements did not specifically highlight the fourth former staff member as having unauthorised access, although an accompanying

data document did. I understand that the witness statements now form part of the ongoing police investigation(s) and, should there be any subsequent criminal proceedings, then they may form part of the evidence.

8. On 29 August 2024, a 'brief facts' document was created by HMCTS Counter Fraud Team which summarised the investigation. That document erroneously interpreted the witness statements above to mean the fourth former staff member's access was legitimate.

9. On 10 October 2024, two former HMCTS staff members were referred to Nottinghamshire police (one former member of staff – from Lewes Crown Court – had already been referred to Sussex police in June 2024). In error, the fourth former staff member was not referred at that point, given that the 22 August 2024 witness statements and the 29 August 2024 brief facts document did not reference their access being unauthorised.

10. On 8 November 2024, HMCTS Counter Fraud Team shared an evidential file based on their whole investigation (including the brief facts document of 29 August, the report of 25 July and the witness statements of 22 August) with Nottinghamshire Police. This package included the 25 July 2024 report, which made comments surrounding the fourth former staff member's unauthorised access, but which were not picked up as part of the witness statements.

11. On 9 April 2025, HMCTS's Delivery Director contacted the HMCTS Counter Fraud Team to confirm that there was a fourth former member of staff who accessed the VC case without business need, having become concerned that they had not been identified as a person of interest in the investigation despite having been identified in the data gathering exercise in July 2024, as per paragraph 6.

12. As a result of this, HMCTS Counter Fraud Team retrospectively referred the fourth former member of staff to South East Regional Organised Crime Unit ('SEROCU'), who had been handed the investigations by Nottinghamshire

Police in December 2024, drawing their attention to them within the evidential file.

13. I understand that SEROCU are investigating this fourth former HMCTS member of staff. I am not aware of the stage at which this investigation has reached and nothing in this statement is intended to prejudice any ongoing investigation. I understand that the police have been in contact with the families of Barnaby Webber, Grace O'Malley-Kumar and Ian Coates, during their ongoing investigations.

14. I apologise on behalf of the MoJ and in particular HMCTS for this important omission from the First Statement.

15. HMCTS has routinely provided placements for interns as part of its Summer Intern Scheme. The induction training provided to interns is the same as the training provided to HMCTS staff, as set out at paragraphs 22 to 24 of the First Statement. Interns also have the same access to HMCTS Job Cards and Key Control Checks. To set up an account on DCS, interns are required to follow the same procedure as set out at paragraphs 18 and 19 of the First Statement (with the clarification below), which includes the signing of online Terms and Conditions (T&Cs).

POINTS OF CLARIFICATION

16. I would also like to clarify the following matters from the First Statement, to assist the Inquiry.

17. Paragraph 18 in the First Statement should read as follows:

For all new users of DCS in roles that can access cases without invitation, a formal registration process is in place which must be scrutinised and approved by Access Co-ordinators (AC) before system access is granted. In addition to this, ACs have assigned responsibilities to regularly monitor access to DCS. For

example, the AC is responsible for running monthly User v Location reports (see paragraph 20 below) and the User Count report to check for continued account eligibility. They also undertake spot checks of case activity and access, using the Record of Case Activity (RoCA) information maintained by the system.

18. This is to clarify that ACs do not need to authorise access for all new users to DCS; they only need to authorise users for roles that require access to cases without specific invitations (e.g. fee-paid judges and defence counsel can access cases on an 'invite-only' basis, so they do not come within Access Coordinator remit). This is also to clarify that the RoCA is not required to be checked monthly, but is available for spot-checking at any time.

19. Paragraph 21 in the First Statement should read as follows:

More generally, DCS maintains a record of all case activity (through the RoCA which logs all user access and document-related actions within cases) and generates an audit trail which is available to all DCS users, with more detailed reports being available upon request from HMCTS Digital Technology Services if required. ACs undertake spot checks of case access / activity using the RoCA information.

20. This is to clarify that a more detailed audit trail of case access is only available through HMCTS Digital and Technology Services, rather than through the RoCA.

21. Paragraph 32 in the First Statement should read as follows:

Further, certain documents can sit within restricted private sections of DCS. Only those documents within a case file which a user is entitled to view will be returned in a search request made by the user. An example of this may be the 'PJ: Private Section - Judge & HMCTS Admin' within DCS to which only members of the judiciary and HMCTS staff with access to that case are permitted to view.

22. This is to clarify that HMCTS staff with access to that case are permitted to view the PJ: Private Section, as well as members of the judiciary.

23. Paragraph 35 in the First Statement should read as follows:

The core probation users of DCS are probation practitioners and administrative staff working in courts to provide reports and advice to the judiciary. Information from the case file available on DCS will in many cases be highly relevant to the preparation of pre-sentence reports ('PSRs'). PSRs provide a professional assessment of risks and needs prepared by probation for the court to make an informed sentencing decision. Where, as set out above, DCS access is aligned to a primary location (usually a user's base) with the option of secondary locations (for courts that they require regular access to), both primary and secondary locations require approval by an access coordinator. The user can automatically access files in their primary and secondary locations. If they try to access files outside of their primary or secondary location, they will be asked to provide a reason for the access and reminded that they should only access case material where there is a business need to do so, and their attention is drawn to the T&Cs of use, access is then automatically granted. The exception of this is when the case record is invitation only; if a user requests access to an invitation only case record, this requires an approved person to review and grant access where appropriate.

24. This is to clarify:

24.1. That access as aligned to primary and secondary locations requires AC approval;

24.2. That access to case record files outside of primary and secondary locations is granted, subject to the user providing a reason for the access (and being referred to the T&Cs of DCS use); and,

24.3. That access to invitation only case record files require a user request which can only be granted by an approved person, following a review and assessment of the user's request.

25. Paragraph 88 in the First Statement should read as follows:

In the UK, personal data processing is governed by the UK General Data Protection Regulation ('UK GDPR', 'the Regulation') and the Data Protection Act 2018 (DPA18). Part 3 of the DPA18 governs the processing of personal data for law enforcement purposes. Where a data breach occurs, the Regulation requires the relevant data controller to notify the data subject whose personal data may have been breached only if the breach "is likely to result in a high risk to the rights and freedoms" of the data subject.

26. This is to clarify the distinction between processing undertaken under the UK GDPR and processing under Part 3 of the Data Protection Act 2018, which governs competent authority processing of personal data for law enforcement purposes.

UPDATES ON IMPROVEMENTS OR ACTIONS TAKEN

27. Since providing the First Statement, there have been developments and improvements in relation to the independent review commissioned into the efficacy and interoperability of relevant policies, titled: 'An independent review into the efficacy and interoperability of MoJ, HMPPS and HMCTS policies in high profile, criminal and contentious cases' ('the MoJ review', 'the Review') **[WITN0065028]**. I discussed the details surrounding the Review, including the issuing, focus, and recommendations, within my First Statement.

28. As part of the Review recommendations, a new process for handling high profile unauthorised access cases has been agreed across HMCTS and MoJ to avoid inconsistencies in the future.

29. The MoJ Personal Data Incident Management Acceptable Use Protocol ('AUP') has also been updated, incorporating lessons learned from the incident. The updated AUP will aim to strengthen accountability for incident management across the department by clearly defining the role of the Data Protection Team ('DPT'). This includes its oversight, advisory, and escalation responsibilities throughout the personal data incident lifecycle. It also sets out the respective roles of the DPT and business areas, clarifying where ownership and accountability sit. The updated AUP remains in draft form and is due to be finalised by the end of March 2026. MoJ will share this with the Inquiry as soon as the final draft has been completed, agreed, and is ready to be implemented.

30. The HMCTS Task and Finish Group (as referred to at paragraph 104 in the First Statement) reported back to the HMCTS CEO and Executive Team in October 2025, setting out some broad options for further exploration. These options ranged from large scale technical system change to a programme of improved culture and awareness across the organisation. In December 2025, the Executive Team asked the HMCTS Digital and Technology Service to develop costed options for delivering technical and cultural change to tackle unauthorised access.

31. This task has been assigned to the HMCTS Chief Technology Officer. So far, a full review of all relevant policies, standards, processes and guidance has been completed. This review has informed the development of a system-access questionnaire, which will provide the data to assess the current controls and lead to the plan of what further access controls need implementing. The HMCTS Chief Technology Officer will update the Executive Team in May 2026, with key findings and next steps.

32. Each of the MoJ review recommendations was assigned to an 'SCS2' Director, a senior leadership position within the Senior Civil Service, to oversee their completion. Many of the actions have already been completed and most of the in-progress actions are expected to be completed by the end of August 2026. As

of March 2026, the conduct policy is still undergoing Trade Union engagement. The anticipated go live date is now June/July 2026.

33. HMPPS has taken action to ensure that only appropriate probation staff have access to DCS, and that use of the system is limited to legitimate business need. HMPPS has worked with HMCTS to tighten the criteria for which probation roles require access to DCS and to refresh the list of probation staff with access in line with this approach.

34. HMPPS has also updated the network of probation ACs for DCS, restricting these roles to Senior Probation Officers ('SPO') and Senior Administrative Officers ('SAO') in court teams. These staff now act as the final arbiters for new DCS account requests from probation staff and have access to new reporting functionality on DCS to ensure only those staff who continue to be eligible for a DCS account have one.

35. This will be supported by new detailed guidance for probation DCS users, which is being finalised for issue shortly. The guidance document will address the rules around who can use DCS, and under what circumstances, provide guidance on how to use DCS, and what to do if something goes wrong, such as a suspected data breach. MoJ will share this guidance with the Inquiry as soon as the final draft has been agreed and is ready to be implemented.

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: 02/04/2026