THE NOTTINGHAM INQUIRY

FIRST WITNESS STATEMENT OF AMY HOLMES

I, AMY HOLMES, will say as follows: -

INTRODUCTION

1. I am, Amy Holmes, interim Director General for the Chief Operating Group[1] of the Ministry of Justice ('MoJ'). I have held this role since September 2025. From March 2025, I was interim Director General for the Service Transformation Group, and previously I substantively held the role of the Public Guardian. I have been a Civil Servant for 25 years and have held multiple senior positions across government.

2. This witness statement is submitted by the MoJ as the parent government department representing the interests of its executive agencies, including His Majesty's Courts and Tribunals Service ('HMCTS') and His Majesty's Prison and Probation Service ('HMPPS'). In this statement I will provide relevant information on behalf of the MoJ and the executive agencies mentioned and will specify when information is provided solely on behalf of one or the other of the executive agencies.

[1] Within the Civil Service, "Group" is the term usually applied to the body of people led by a Director General (Senior Civil Servant ("SCS") pay band 3). Groups are sub-divided into Directorates, each of which is led by a Director (SCS pay band 2). Directorates are sub-divided into Divisions, each of which is led by a Deputy Director (SCS pay band 1).

3. I am duly authorised to make this statement on behalf of the MoJ, HMCTS, and HMPPS. I believe that the facts stated in this witness statement are true. In preparing this statement, I am reliant upon the work of officials in HMCTS Operations, HMCTS Service Team, HMCTS Communications Team, the HMCTS Counter Fraud Team, and the MoJ Security and Information Directorate ('SID'), which includes the MoJ Data Protection Team ('DPT'), as well as the work of officials in HMPPS East Midlands region, Probation Operations, and Corporate Services. MoJ, HMCTS, and HMPPS officials have coordinated and liaised with colleagues that have relevant knowledge and experience across HMCTS, HMPPS, and the wider MoJ; their contributions have been used for the purposes of preparing this statement. My statement therefore relies upon those contributions and not all matters within this statement are necessarily from my own personal knowledge or recollection.

4. This statement is made to assist the Nottingham Inquiry ('the Inquiry') and in particular addresses any unauthorised access and/or disclosure of case files and evidence by HMCTS and/or HMPPS staff, following Valdo Calocane's ('VC') arrest on 13 June 2023, including, if relevant, the handling of and communications with the survivors and bereaved families.

5. This statement is provided to the best of my knowledge and belief, upon taking advice and direction from MoJ, HMCTS, and HMPPS officials and is accurate and complete at the time of signing and whilst the MoJ, HMCTS, and HMPPS continue to prepare for this Inquiry.

BACKGROUND

Organisational architecture

6. HMCTS is an executive agency of the MoJ and reports to the MoJ. It was established on 1 April 2011 through the merger of Her Majesty's Courts Service, and the Tribunals Service. Since this time HMCTS has been responsible for

providing the system of support, including infrastructure and resources, for the administration of the business of the courts in England and Wales and those tribunals throughout the United Kingdom for which the Lord Chancellor[2] is responsible. HMCTS provides the support necessary to enable the judiciary, tribunal members, and the magistracy to exercise their judicial functions independently.

7. Reflecting the constitutional settlement safeguarding the independence of the judiciary, HMCTS is not a conventional executive agency. Rather, HMCTS operates through a partnership between the Lord Chancellor, the Lord/Lady Chief Justice of England and Wales ('LCJ')[3], and the Senior President of Tribunals. This partnership is underpinned by the Constitutional Reform Act 2005 and governed by a 2014 Framework Document under which day-to-day operational management is delegated to a Chief Executive under the general direction and strategic leadership of the HMCTS Board, which has an independent chair.

8. HMPPS is also an executive agency of the MoJ and reports to the MoJ. In April 2017, HMPPS replaced the National Offender Management Service ('NOMS'), with the intention of creating a more operationally focused organisation. The agency is comprised of HM Prison Service, The Probation Service, The Youth Custody Service, and a headquarters focused on supporting frontline operations.

---

[2] The Lord Chancellor is appointed as Lord Chancellor and Secretary of State for Justice, and heads the MoJ, which covers both Lord Chancellor responsibilities and Secretary of State responsibilities.
[3] The LCJ's duties include, but are not limited to, judicial deployment, training, and guidance for the judiciary, and representing the views of the independent judiciary to the Lord Chancellor and Ministers of the Crown. Judges are also responsible for the allocation and listing of cases, not HMCTS. These responsibilities are outlined in the Constitutional Reform Act 2005 and Concordant. The Concordat is the recognised shorthand for a document called "Constitutional Reform. The Lord Chancellor's Judiciary-Related Functions: Proposals." It was placed in the libraries of both Houses of Parliament in 2004. The text was also printed as Appendix 6 to the House of Lords Constitutional Reform Bill – First Report which was which was ordered by the House of Lords to be printed 24 June 2004. It outlines the modification of the role of the Lord Chancellor and the transfer of that post's judicial functions to Lord Chief Justice for England and Wales.

9. HMPPS plays a crucial role in society in ensuring the implementation and facilitation of sentences given by the courts, both in custody and in the community, and rehabilitating people in its care by addressing education, employment, accommodation, health, and substance misuse needs. Within England and Wales, HMPPS is responsible for: running prisons and Probation Services, rehabilitation services for people in its care leaving prison, making sure support is available to stop people reoffending, and contract managing private sector prisons and services such as the prison escort service and electronic tagging.

10. The MoJ's DPT supports the entire MoJ family, including HMCTS and HMPPS. The DPT drives the Department's data protection strategy and provides training, advice and general support. The Data Protection Officer (DPO), a statutory role, sits within the DPT, which is part of SID.

11. The DPO, through the DPT, is responsible for reporting to the Information Commissioner's Office ('ICO') and data subjects. The DPT reviews and assesses any potential data breach to determine whether the incident reaches the threshold for reporting. Where an incident is assessed as reaching the reporting threshold, the DPT is responsible for making a report to the ICO. If it is deemed necessary, they will notify data subjects, and this is usually done by the team with the closest relationship to them.

12. The MoJ is the data controller for all personal data processing carried out by HMPPS and HMCTS. This is covered within the MoJ's formal registration, as a data controller, with the ICO.

Operating system for accessing case files and evidence

13. This section of my statement deals with the operating systems for accessing case files and evidence, and relevant guidance in existence at the time of the unauthorised access.

14. The relevant operating system used for the holding of case material in this matter, and which is accessible by certain staff from both HMCTS and HMPPS, is called the Crown Court Digital Case System – CCDCS. For ease I shall refer to the system as 'DCS', which is how it is commonly referred to within the criminal justice system.

15. HMCTS operate DCS as well as a second digital system, operational since July 2023, known as the Common Platform ('CP'). This is in addition to the 'legacy' case management system in the Crown Court known as 'Xhibit'. CP is now the principal system of record and is used to administer cases from start to finish. Rollout of CP commenced in September 2020 and went live in all criminal courts in July 2023. As of April 2025, approximately 85% of all Crown Court work is initiated on CP, whilst the remaining 15% is initiated on Xhibit. This 15% includes some prosecutors (including those bringing private prosecutions) not yet using CP and some older cases in Crown Courts that are still managed via legacy case management systems.

16. Although the CP Case Material function is used to save and store documentary information for cases in the magistrates' court, save for the 'Initial Details of the Prosecution Case' document (which is a document containing information necessary to effectively progress cases at the first hearing including; a list of the charges/offences, a summary of the prosecution evidence and/or copies of key witness statements, record of interview, list of exhibits, and Defendant's PNC (Police National Computer) record), neither CP nor its Crown Court legacy system Xhibit, are used to handle or store documentary evidence for Crown Court purposes. That function is fulfilled by DCS. HMCTS has produced online guidance to assist DCS users when uploading documents to DCS. The guides explain which sections of DCS each document type should be added to, who is

responsible for uploading documents in each section, and which sections are restricted to certain parties **[WITN0065002 and WITN0065003]**.

17. DCS is a web-based software solution that enables multiple individuals to upload and access case information. This includes members of the judiciary, parties to the case, and other individuals involved in Crown Court proceedings, such as relevant Criminal Justice System (CJS) partner agencies like the Crown Prosecution Service (CPS) and Probation Service. DCS facilitates the preparation, presentation, and sharing of documentary case papers, including evidence, in a digital format. The lifecycle of a case on DCS includes various stages from the initial file set up (following sending/committal to the Crown Court) to activity in relation to the management and conduct of appeals **[WITN0065004]**.

18. For all new users of DCS, a formal registration process is in place which must be scrutinised and approved by Access Co-ordinators (AC) within HMCTS 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) and for doing monthly spot checks of case activity/access (using the record of case activity – 'RoCA' – information maintained by the system).

19. To access the DCS generally an account must be set up linked to an email address which is for a domain recognised by DCS (e.g. @justice.gov.uk). Once an account is set up, online Terms and Conditions ('T&C's') must be signed by all system users. The first term to agree is *"I have a legitimate need to use Crown Court DCS and will only access case material where I have a business need to do so"* **[WITN0065005]**. Further terms of relevance include a requirement to comply with the Data Protection Act 2018 and to only access the service from devices which have appropriate enabled security controls installed.

20. The system also contains a prompt when a user attempts to access a case outside of their assigned work location(s). When doing so, the user must input a business reason/need for the access **[WITN0065006]**. This information then feeds into the User v Location Reports that ACs are expected to run monthly (as mentioned above). The AC will use the reports to identify any signs of unusual case access outside of their location. They will follow up those checks by speaking to individuals concerned (or alerting others to suspected inappropriate access), and then, where appropriate, follow internal guidance on information security and counter fraud reporting to escalate any issues as required. Only an AC can run a User v Location report (see paragraph 30) **[WITN0065007 and WITN0065008]**.

21. More generally, DCS maintains a RoCA which logs all user and document-related actions within cases) and generates a detailed audit trail which is available to all DCS users, ACs, as part of Standard Operating Controls in court, undertake monthly spot checks of case access/activity using the RoCA information.

22. All HMCTS staff users have access to user guidance available on the staff intranet **[WITN0065009, WITN0065010 and WITN0065011]**. At the relevant time, users had access to a guidance document published on 31 July 2019. The 2019 guidance defines a 'business need' to access a case as - when the work a user has been allocated by their line manager *"requires you [the user] to complete an activity on DCS"* or *"use information stored on DCS"* to *"assist you [the user] in carrying out your duties."* It outlines what acceptable use of the DCS is and explains what the consequences of failing to adhere to these requirements are.

23. Further to the DCS T&Cs and online guidance, HMCTS operates a system of Job Cards and Key Control Checks ('KCCs') which set out the processes for staff to follow and the associated compliance checks to be carried out, for example the *Job Card: Audit of Crown Court Digital Case System (DCS) File*

Access Procedures **[WITN0065012]**. Guidance and training material is also provided to all DCS users (including both HMCTS and HMPPS users) via GOV.UK webpages **[WITN0065013]**.

24. The DCS T&Cs also requires all users to "inform the Crown Court DCS Helpdesk prior to leaving my role in order that my account may be deleted." General staff management processes provide that all managers are responsible for following a leavers checklist when staff leave the department **[WITN0065014]**. This checklist includes an action to remove HMCTS system access, including DCS access. Local Digital Support Officers ('DSO') report monthly to ensure courtroom and IT equipment checks are being carried out, which includes a check on the removal of system access for staff who have left the court thereby minimising the risk of unauthorised access by any leavers.

25. Whilst not specific to DCS use, HMPPS and HMCTS staff, including frontline court and probation staff are required to undertake training every 12 months under the Civil Service Learning Module: "Security and Data Protection Fundamentals". This training includes:

25.1. understanding data types and protection principles;

25.2. protecting assets, personal data, and the business from security threats;

25.3. responding to security incidents and operating safely online; and,

25.4. recognising phishing attacks and taking appropriate action.

Restricting access to case files

26. As explained above, DCS is a system which provides access to case documentation for a wide range of user types across the criminal justice system when involved in criminal proceedings.

27. HMCTS administers and supports the work of the criminal courts in a manner that requires considerable flexibility. This way of working is required because in any one court location, multiple clerks and other court administrators will routinely have a legitimate business need to work on/deal with a case. Administrative support is often clustered across neighbouring court centres for efficiency, and increasingly, HMCTS is effecting inter-regional transfers of cases to try to meet the outstanding caseload backlog challenges.

28. Within HMCTS, intra and cross-court access is a regular, and essential part of case management and administration; cases might be worked on by several individuals in the course of proceedings, and several court clerks might be called upon to undertake hearings as the case progresses. Cases might also be moved between court centres (and/or judges) in the interests of timeliness. In addition, general contact (e.g. media queries about cases) are also handled in a limited number of national Court & Tribunal Service Centres. This means that the tighter access controls in place, the more strain is put on the efficiency of the service provided. The ability for more than one individual to access case material is also an integral part of other agency/professional ways of working (e.g. within the CPS and across the defence/prosecution professions).

29. There are some existing controls built into DCS to help manage access, such as the functionality to mark a case as sensitive so that access is only granted on an invitation only basis. Staff from non-HMCTS/CPS/probation agencies and counsel are invited to access the case in the first instance, so there is a degree of up-front control. As a case progresses, it is possible for more/new non-HMCTS individuals to be given case access as the case may require.

30. DCS staff users in HMCTS can be assigned a primary and a secondary location (usually their main court base and any other on whose cases they might routinely work on). A user does not need to justify their reasons for accessing a particular case assigned to their location. Where a staff user attempts to access a case outside of their primary or secondary location, they are prompted to enter into a free text box, a justification for doing so. The reasons entered at this point will be captured in the User v Location reports which ACs are required to run monthly. These reports identify which cases have been accessed by users outside of their primary or secondary location. It is important to note that a Nottingham AC, running a User v Location report would only be able to identify 'out of area' cases which have been accessed by someone with Nottingham as either primary or secondary location. It could not be used to identify where a Nottingham user might have inappropriately accessed another Nottingham case. A Nottingham-based AC would not be able to identify a DCS user outside of their primary or secondary location who has inappropriately accessed a Nottingham case, for example a Luton Crown Court clerk, who has accessed a Nottingham case. However, the AC at Luton Crown Court, running their User v Location report, would be able to identify the clerk's accessing of the Nottingham case.

31. In addition, DCS is constructed in a way that means that users are only able to access the information necessary to perform their duties (determined by user role). For example, HMCTS users (and the judiciary) are unable to access documents which have been uploaded onto DCS in accordance with the CPS's ongoing duty of disclosure, but which are ultimately not going to be used, or relied upon by the prosecution as part of their case. This material is referred to as unused material and is stored in a section of the DCS only visible to the prosecution, defence, and read only users.

32. 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

judge's private section within DCS to which members of the judiciary with access to that case will only be permitted to access document uploaded to that section.

33. Whilst these controls are robust, HMCTS must undertake a risk based balancing exercise to protect access to case information but also support efficient business processes, both of which have a real public interest. It is therefore acknowledged that the system does not entirely prevent staff from viewing information that they technically have access to, even if they do not have a valid business need to view it. To mitigate this, HMCTS have in place the said terms of use to limit staff access strictly to those who require it for business purposes, and there are processes in place to ensure that accounts are disabled when access is no longer required.

34. Where HMCTS staff are found to have accessed material without a business need to do so disciplinary action is taken. This may result in a finding of gross misconduct and dismissal. In such cases, in line with the HMCTS Counter Fraud Policy and Response Plan, the police are also invited to investigate.

35. 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 provides for restrictions from accessing material beyond a particular region then this might be an example of when a registered user might need access to a case for a business area to which they might not have access. If this is needed then they must request access, and they are reminded that they must only access case material where there is a business need to do so, and their attention will be drawn to the T&Cs of use.

36. For cases involving special sensitivity, additional access restrictions can be applied. On 10 May 2021, 'Invite Only' functionality was introduced to DCS, along with a supporting Job Card explaining the functionality, when it might be appropriate to be used, and how to use it **[WITN0065015]**. This functionality can be activated following notification from the magistrates' court, unilaterally by court staff, upon representation from defence/prosecution, or as a result of judicial direction or order. For example, the CPS may verbally state at the initial magistrates' court hearing that the case is sensitive, and this will be noted by the legal adviser in the relevant section of the Better Case Management Form ('BCM'). Where there is a difference of opinion about the sensitivity of a case, and the consequential need for access restrictions, the route for escalation is to refer the case to a judge for determination.

37. It is possible to activate, or deactivate, 'Invite Only' functionality at any time and this feature restricts access to named users only. Use of this function means that other individuals cannot access the case. If a user who is not invited attempts to access the case, they will be unable to do so and will be presented with a list of users who do have access who can be contacted to either carry out the required task or assess whether access should be extended. Where there is a legitimate business need to extend access then this can be set up for a specified period, or indefinitely, dependent on the nature of the task for which access is required. The 'Timed Invitation' functionality allows an expiry date to be set when a user is invited into a DCS case. Once a date is set using this functionality, the user may access the case at any point up to the expiry date but is removed from the case after the date elapses.

38. Given the DCS T&Cs and supporting guidance, it was not felt necessary to restrict access at the point at which the VC case was uploaded to DCS. At the time, the case was proceeding to hearings and required many actions to take place – i.e. uploading documents, responding to press enquiries, requests from judges for information, public engagement, submission of reports and so on. The case was restricted to invite only on 23 May 2025.

39. In respect of the specific geography in this case, probation access to DCS was restricted to the Nottinghamshire Court area. In practice, this meant only court-based Probation staff and those in victim liaison roles in the East Midlands Probation Service ('EMPS') Nottinghamshire region had access to DCS. The grades and roles of staff included:

39.1. Probation Service staff working in Nottingham Crown Court to provide reports to the judiciary:

39.1.1. Senior Probation Officers (SPO). SPOs are the first-line management grade within probation.

39.1.2. Probation Officers (PO). POs, together with PSOs, make up the core frontline grades of operational staff in probation and are qualified to supervise high-risk cases. In court, both grades of staff are responsible for producing pre-sentence reports and other information for judges.

39.1.3. Probation Service Officers (PSO). POs, together with PSOs, are the other main frontline operational grade in probation.

39.1.4. Case Administrator (CA). CAs provide administrative support to probation court teams and other probation functions.

39.2. Victim liaison staff:

39.2.1. Victim liaison case administrators ('VLCA'). VLCAs provide administrative support to probation victim liaison teams, who keep victims of serious sexual and violent offences informed about key developments in the offender's sentence.

40. Additionally, access included Case Administrators within Mansfield Magistrates' Court. The DCS platform is used by probation in this and other regions for analysis of court lists to anticipate requests for information or reports, downloading documents to inform the preparation of PSRs, uploading PSRs, checking for next court dates, and for sentencing remarks which may inform work towards a convicted offender's future Parole Board hearing.

41. Upon sentencing, certain documents of relevance to probation managing the offender's sentence will be extracted and added to the probation case management system called N-DELIUS. This would include any offence history set out in the case files and might include details of how an offence was committed (for example, if a weapon was used) that would be relevant to future assessments of the offender's risk. HMPPS operates a Limited Access Policy for high profile cases within their own document recording system called N-DELIIUS **[WITN0065016]**.

42. From the perspective of HMPPS, the work to assess and manage offender risk is conducted on a case-by-case basis, having regard to all the circumstances within the case. This makes an overarching set of rules or policies for every eventuality challenging. However, the safeguard in place was to ensure that only staff in specific roles could access material on DCS and those who did understood that access was for legitimate business need only.

43. When HMPPS receives information that there has been an alleged unauthorised access, HMPPS's 'conduct and disciplinary' processes are followed, as set out in the policy framework document "PI 34 2014 – Conduct and discipline". The first step of the process involves a fact-finding exercise, which is followed by a further investigation, should it be required. The outcome of any investigation may result in a hearing to determine the finding and penalty. Referrals would also be made to HMPPS's Counter Corruption Unit and SID, for further consideration and advice. The 2014 policy framework document was in force at the time of the unauthorised access in this case **[WITN0065017]**.

44. In this case, HMCTS followed the MoJ Conduct and Discipline Policy and determined the access by some staff was inappropriate and took formal disciplinary action in line with the policy. The MoJ IT usage guidance, that forms part of the Conduct and Discipline Policy, stipulates that misuse of the MoJ IT systems will be treated as a disciplinary matter, with the potential of possible dismissal. HMCTS did not recognise the incident as a personal data breach and, accordingly, did not inform SID.

45. Similarly, in addition to taking action under the Conduct and Discipline Policy, HMPPS's approach was additionally informed by the National Probation Service Conduct and Discipline Guidance **[WITN0065018]**. Following preliminary investigations under this policy, HMPPS found no basis for formal action against their staff. Instead, advice and guidance were provided to HMPPS staff in relation to accessing court records.

DATA ACCESS IN THIS CASE

46. The crimes perpetrated by VC occurred on 13 June 2023. The case was first received by Nottingham Magistrates' Court, by way of a Case Summary document (MG5), Charge Sheet (MG4), and the Initial Details of the Prosecution Case (IDPC) on 16 June 2023. These documents were uploaded onto CP, not DCS, as is standard process in all new cases received by the magistrates' court. In addition to the MG4 and MG5, the IDPC contains police and civilian witness statements. At this point, the information uploaded to CP would not usually contain photographs, CCTV footage, or other forms of evidence (above the witness statements).

47. Following charging of a suspect, it is usual for the matter to come initially before the magistrates' court for a first hearing. In this case that first hearing took place

at Nottingham Magistrates' Court on 17 June 2023, and the case was then sent to the Nottingham Crown Court on the same date.

48. The case was received at Nottingham Crown Court and booked into the DCS system on 19 June 2023 by an Administrative Officer[4]. The evidence booked into the DCS included a CCTV working document, a document containing still images of comparison and identification of an image of the weapon used by VC, and the MG5. From this point, the DCS case was accessible to all HMCTS, CPS, Probation Service staff, and Judiciary with DCS access. This is designed to allow further updates to the case to be added or documents uploaded in real time, to administer future hearings and to check the case for incoming enquiries for example, from the public, press, and legal representatives.

49. Permission to allow DCS access for defence representatives is granted by HMCTS to the solicitors named on the Representation Order (or to the solicitors that represented the defendant in the magistrates' court if no Representation Order is received). In this case VC's solicitors was Bhatia Best Solicitors and access was granted on 19 June 2023.

50. A typical Crown Court case can include information with a number of different levels of sensitivity, such as personal identifiable or commercial information. In this case, the CPS uploaded further information onto DCS from June 2023 to January 2024. In terms of images and video footage, images of the defendant, and a document that provided a timeline of still images of the CCTV (called the CCTV Working Document), and Scene of Crime Officer (SOCO) and photo evidence, were uploaded by the CPS on 18 August 2023. A CCTV sequence of events file was uploaded on 2 October 2023. Later that same month on 24 October 2023, a sequence of events document was uploaded and on 21 November 2023 and 22 December 2023, some further images were uploaded.

---

[4]

51. From October 2023 to January 2024, further prosecution and defence documents were uploaded to DCS. These included seven psychiatric reports uploaded by the defendants' solicitors and the CPS uploaded between 2 October 2023 and 22 January 2024. Three reports prepared by the expert instructed by the defence were uploaded by a Bhatia Best Solicitors on 21 November 2023, 13 December 2023 and 22 January 2024. Two reports prepared by the expert instructed by the prosecution were uploaded on 24 November 2023 and 17 January 2024.

52. Other documentation was uploaded throughout the lifecycle of the case; a full list can be provided and detailed if required. However, the items listed above are considered the most sensitive documents uploaded to DCS, including, but not limited to, a large volume of personal data, images of crime scenes, statements containing graphic details of the offences, and pathological evidence.

53. In terms of CCTV or other video footage, save in those instances where still, and sometimes graphic, pictures have been captured from moving footage, in which case the access controls previously outlined in this statement apply, DCS is unable to directly hold video or audio material. Instead, such material is shared via secure Digital Evidence Management Solutions ('DEMS'), and is managed by either the police or the CPS, and not HMCTS, HMPPS, or the MoJ.

54. The process for providing access to CCTV, other moving footage, or audio material typically involves the prosecution embedding a secure web link to the video or audio evidence within a document that is then uploaded to DCS. This allows the judiciary, defence, and instructed advocates to access the material directly through the DEMS platform. The protocols governing who can register for and access DEMS links are managed entirely by either the police or the CPS, and not HMCTS, HMPPS, or the MoJ.

55. HMCTS staff working in the Crown Court are not routinely registered for DEMS accounts or access multimedia evidence, as it is not required for the

performance of their duties. This means that HMCTS staff cannot access or view this type of evidential material. I have been advised by HMPPS and HMCTS that none of the staff under investigation had accessed video or CCTV footage.

56. There is a limited exception to this rule in the Court of Appeal. In the Court of Appeal, a small number of HMCTS-employed lawyers are permitted to access video or audio evidence to support the judiciary. This access is restricted to material that has been transferred to the Court of Appeal workgroup within the CPS-managed DEMS platform, Egress, and applies to very limited and specific situations. As one would expect, the Court of Appeal deals with far fewer cases.

57. As of 24 June 2025, 106 HMCTS and non-HMCTS users, have accessed this case on DCS. These users can be broken into the following user's groups:

57.1. HMCTS staff – 22

57.2. HMCTS Court of Appeal Staff (Royal Courts of Justice) – 13

57.3. CPS staff – 22

57.4. HMCPSI (His Majesty's Crown Prosecution Service Inspectorate) - 4

57.5. HMPPS Probation Service staff – 11

57.6. Judiciary – 9

57.7. Defence Advocates and Clerks – 17

57.8. Prosecution Advocates and Clerks – 8

58. It does not automatically follow that those who accessed the case on DCS accessed the most sensitive material. There are legitimate reasons why a user

would need to access a case 'at-a-glance', for example, when answering a media enquiry about the date of a future hearing. A user could access certain information on the case to answer this type of query without any need to view sensitive information like CCTV stills or photo evidence. The list of 106 DCS users who have accessed this case simply represents basic access and is not representative of access to sensitive data, information, or material.

59. Turning to the alleged unauthorised access by HMCTS and HMPPS staff to sensitive data and management of the same, the following provides a summary of events in relation to each agency:

HMPPS

60. On 25 January 2024, the court SPO was contacted by the Delivery Manager at Nottingham Crown Court regarding inappropriate access to DCS by one member of its staff. To HMPPS's knowledge this is the first time that access to DCS by their operatives had been questioned by Nottingham Crown Court. The Delivery Manager, following Standard Operating Checks in court, using a RoCA report, identified HMPPS staff accessing the VC case, and assessed that they could see no obvious business need for them to have done so.

61. On 29 January 2024, further information was provided to EMPS Nottinghamshire regarding the remaining members of staff who had accessed the VC case. EMPS were provided with a list of nine further names of probation staff by the same Delivery Manager at Nottingham Crown Court.

62. In addition to the ten probation staff whose access was queried by the Crown Court Delivery Manager, the eleventh member of probation staff referenced as having accessed this case on DCS was the Court SPO to whom the referral was made. The SPO, although initially referenced, was quickly discounted and accepted as having a legitimate reason to access DCS, given that access to this

case would have been fully in line with their senior probation role within the court setting.

63. Of the remaining ten, and following liaison between the Probation Service and HMCTS, there was agreement that two PSO's and one VLCA had clear rationale for accessing the case, which was in line with their specific probation roles within the court setting. PSOs access relates to reviewing court listings and preparing for possible requirements for pre-sentence reports. VLCA access relates to reviewing court dates ready to engage with victims under the victim contact scheme.

64. This left seven members of probation staff remaining within scope of further enquiries around their access of the case:

64.1. HMPPS staff member (1) (CA) - access on 20, 21 and 26 June 2023

64.2. HMPPS staff member (2) (PSO) – 20 June 2023

64.3. HMPPS staff member (3) (PSO) – 20 January 2024

64.4. HMPPS staff member (4) (CA) – 19 June 2023

64.5. HMPPS staff member (5) (PSO) – 23 January 2024

64.6. HMPPS staff member (6) (CA) – 25 January 2024

64.7. HMPPS staff member (7) (CA) – 26 January 2024

65. For these remaining seven members of probation staff (four CAs and three PSOs) a process ensued to establish the facts of the case access, which involved the SPO speaking to each of the individuals. For the four remaining

CAs, their rationale for case access was accepted to be in line with expectations of their role in the court setting, and no further action was therefore taken. For the three remaining PSOs, it was found that despite each officer not having clear grounds for access to the case, in line with probation expectations, their actions did not trigger a further conduct and disciplinary formal investigation. Disciplinary proceedings were not taken any further, and the findings from the preliminary investigations led senior probation staff to resolve the matter internally through the issuing of formal improvement actions. From an HMPPS perspective, the probe into staff who had their access queried was dealt with proportionately and in line with HMPPS conduct and disciplinary policy, and the cases were subsequently closed. The further subsequent police referrals of HMPPS staff were triggered by HMCTS's Counter Fraud Team, based on that Team's investigatory thresholds.

66. In January/February 2024, the preliminary investigation into the access took place, led by the SPO, who was the line manager of the Probation Service Officers. This included liaison with HMPPS senior managers and the HMPPS Counter Corruption Unit and found that there was no apparent malicious intent or personal gain in reference to the staff involved. The conclusion agreed by the Head of Service was as follows:

66.1. All three members of staff received the same outcome, agreed by Head of Service and communicated to the individuals by the line manager. The rationale being that all three were relatively new in post and in their training period;

66.2. HMPPS staff member (1) (PSO) – in post for ten weeks at the time of accessing,

66.3. HMPPS staff member (2) (PSO) – in post for six weeks at the time of accessing, and

66.4. HMPPS staff member (3) (PSO) – in post for just over six months at the time of accessing.

67. HMPPS took the following actions following the outcome of their preliminary investigations:

67.1. Individual conversations took place with staff members by the East Midlands Counter Corruption Lead.

67.2. A specific Counter Corruption briefing was delivered to all probation staff based at Nottingham Crown Court reminding them of their responsibilities with regards to accessing information, ensuring they fully understood their obligations under their terms and conditions, and fully refreshed reminders on what staff can and cannot do.

68. The referrals made by HMCTS to Nottinghamshire Police, in May 2024, were known to HMPPS. The Probation Service were informed that HMCTS had referred the matter to Nottinghamshire Police and met with Nottinghamshire Police, alongside HMCTS, to discuss the access and the actions taken internally. Nottinghamshire Police determined that this referral would not result in an investigation. This information was communicated by Nottinghamshire Police to HMPPS on 9 June 2024, by email.

69. On 8 December 2024, HMPPS received notification from the South East Regional Organised Crime Unit (a policing unit known as 'SEROCU'), via an email sent to the East Midlands Probation Service Strategic Lead for Courts, that they were launching an investigation into this matter. A further notification was sent by SEROCU to the Head of Service for Nottinghamshire on 11 December 2024.

HMCTS

70. Following the initial identification of possible unauthorised access by the HMCTS Delivery Manager in January 2024, as well as reporting to the Probation Service, the Head of Service reported the incidents to the HMCTS Data Incidents Team (30 January 2024). That same day, in line with usual practice when logging cases involving potential fraudulent or criminal activity, the Data Incidents team referred the matter to the HMCTS Counter Fraud Team.

71. The Counter Fraud team's investigation into the ten HMPPS staff's access of DCS began on the 1 February 2024. On the 14 May 2024, the HMCTS Chief Information Security Officer (CISO) informed the HMPPS Senior Information Risk Owner (SIRO) and MoJ Chief Security Officer (CSO) of the intention to refer seven of these staff members to the police. On 21 May 2024, referrals to Nottinghamshire Police were made.

72. As part of these investigations, the Counter Fraud Team requested numerous Audit Logs of user activity on DCS. Subsequently, and as a result of reviewing these Audit Logs, on 16 May 2024, the Counter Fraud team begun investigations into HMCTS staff unauthorised access of DCS records in this case. These further investigations identified three members of HMCTS staff; two based at Nottingham Crown Court and one based at Lewes Crown Court, who had accessed the case without clear business need. There was a concern that these accesses were inappropriate and unauthorised. They can be summarised as follows:

72.1. HMCTS staff member (1) (Crown Court clerk) – Nottingham Crown Court – 18 January 2024

72.2. HMCTS staff member (2) (Crown Court usher) – Nottingham Crown Court – 23 January 2024

72.3. HMCTS staff member (3) (Administration Officer) – Lewes Crown Court – 19 June 2023

73. In October 2024, following the Counter Fraud Team's investigation of the three HMCTS staff, a further evidential file was submitted to SEROCU (in respect of the Nottingham members of staff) and Sussex Police (in respect of the Lewes member of staff) with the details of HMCTS staff inappropriate access to court records on DCS.

74. In addition to the police referrals, these Counter Fraud Investigations triggered disciplinary action (under the MoJ HR policies) against two HMCTS employees, as a result of which both are no longer in the employment of HMCTS **[WITN0065019]**. The third HMCTS employee resigned shortly after the unauthorised access was identified.

MoJ DPT

75. On 29 January 2024, the MoJ DPT received an email notification from the SPO based at Nottingham Crown Court regarding inappropriate access to DCS.

76. On 30 January 2024, due to the limited amount of information provided, and to determine the severity of the incident, the DPT requested further information. This included:

76.1. The exact nature of the information that was inappropriately accessed;

76.2. How many staff in total had accessed the information;

76.3. If any of the information had been downloaded, copied or printed;

76.4. The status of those staff and their access to systems;

76.5. Details of any further investigations; and,

76.6. Had the incident been escalated within the relevant HMPPS incident reporting structure.

77. A response to this request was received from the SPO on 31 January 2024. Based on the information provided, the DPT did not assess that the incident warranted an incident review panel. The MoJ Information Security Team ('MIST') were informed of the incident for awareness. SID did not progress an investigation into the incident at this time as HMPPS were completing their investigation.

78. On 13 December 2024, SEROCU wrote to the Head of Nottingham PDU to inform them of the criminal investigation. This was escalated to the HMPPS SIRO who informed the MoJ's CSO, the DPO and the HMPPS Director General Chief Executive Officer (CEO), in the absence of the HMPPS Director General (DG). On 14 December 2024, the DPO wrote to the HMCTS CISO to inform them of this development. On 16 December 2024, the DPO informed the HMCTS CEO of the incident.

79. On 17 December 2024, the HMCTS CEO and the HMPPS DG, informed the Permanent Secretary of the inappropriate access. The briefing proposed the MoJ SID conduct an independent review into the efficacy and interoperability of relevant policies. On 16 January 2025, the DPT wrote to the police, as requested by the Permanent Secretary, to inform them of the review and its scope, and provided reassurance that it would not interfere with their investigation.

80. On 20 January 2025, following approval from the police, the Permanent Secretary commissioned the review. The purpose of the review was to ensure that the MoJ, and its agencies, had appropriate policies and processes in place when handling matters when there is an allegation or suspicion of potential illegal activity on the part of employees or contractors. The review excluded any

action that could interfere with, or prejudice, the ongoing police investigation and/or any subsequent criminal proceedings.

81. When the DPT are made aware of a personal data incident the team will carry out an initial assessment of the incident. If the incident is assessed to be high/substantial in severity, it is escalated to a senior member of the DPT who will convene and incident review panel. An incident review panel is comprised of at least one member of the Office of Data Protection Officer (usually the MoJ DPO and a Deputy DPO), Data Protection Strategic Leads, and Data Protection Managers. The panel will discuss whether the incident in question meets the threshold to notify the ICO **[WITN0065020]**.

82. On 23 April 2025, the DPT agreed to convene an incident panel, following the commissioning of the independent review, and further scrutiny of the case by HMCTS, HMPPS, and MoJ. When the incident was first reported to the DPT in January 2024, given the limited information available at the time, and the ongoing HMPPS investigation, the DPT initially determined that an incident panel was not required.

83. At the panel in April 2025, the DPT concluded that although the access to the records constituted a data breach, it did not meet the threshold for reporting to the ICO or the victims, victims' families, or the offender. The DPT assessed the risk to individuals was low given that there had been limited access to personal data, some of the information was already available publicly (the case was held in open court and widely reported in the media), and it had not been extracted from the systems or shared onwards.

84. More generally, I am not aware of any information or allegation that suggests that anyone from the MoJ, HMCTS, or HMPPS referred to any information or material held on this case in any inappropriate telephone messaging with any other individuals, agencies, or externally.

STEPS THAT COULD OR SHOULD HAVE BEEN TAKEN TO PROTECT THE INTEGRITY OF THE DATA AND THE DIGNITY OF THOSE IMPACTED.

85. In this case, I am advised that the view of HMCTS is now that earlier consideration should have been given to the sensitivity of the case and that the 'Invite Only' functionality should have been applied earlier. Had the case been so identified, access to the case material would have been restricted to specifically invited individuals with a verified business requirement.

86. HMPPS relies on the application of broader system-usage policies and training for staff to then be put into context when staff are using DCS. The HMPPS consider that whilst consistent guidance has been issued across the East Midlands probation region, HMPPS would benefit from more consistent management oversight of how probation staff learn to use DCS, and taking steps to ensure that HMPPS staff who are required to access DCS are aware of broader information management rules and are clear on how they apply to usage of DCS. Their view is that this would help to protect the integrity of data and the dignity of those affected in the future.

INFORMING THOSE IMPACTED BY UNAUTHORISED ACCESS TO CASE FILES

87. The MoJ is the data controller for HMCTS and HMPPS data. HMCTS/HMPPS identify and then escalate personal data issues to the MoJ, and MoJ decide whether to report or act on a personal data breach.

88. In the UK, data protection is governed by the UK General Data Protection Regulation ('UK GDPR', 'the Regulation'). Where a data breach occurs, the Regulation requires the relevant data controller to inform 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.

89. The investigations into the unauthorised access in this case revealed there was no evidence that the personal data accessed had been shared with any other persons. The MoJ, acting as the data controller, is legally obligated to inform the data subjects only where there is a "high risk". The Department is legally obligated to inform the ICO where there is a "risk" to data subjects. Incidents involving the inappropriate access of case records, even where the case is high profile, do not automatically meet the threshold of "risk" or "high risk."

90. It is the role of the data controller to consider and assess the risk of harm to the data subjects whose personal data may have been breached. It was determined that the incident did not meet the requirements under UK GDPR Article 33 or Article 34 to report the personal data breach to the ICO, or the data subjects.

91. It is imperative, when conducting internal investigations which consider the requirement for referral to the police for consideration of criminal investigation, that a clean chain of evidence is prioritised. Communication regarding the existence or substance of suspected unauthorised access where there is a risk that such communication may prejudice the ongoing police investigation, should be approached with caution. It is also inappropriate for there to be any further comment on criminal investigations and court proceedings, whether the relevant agencies referred to in this statement are a party to those proceedings or not.

92. It is usual for the police to liaise with victims and witnesses in relation to criminal investigations and court cases. Victim liaison is not usually a function of HMCTS or MoJ HQ.

93. Due to the nature of probation work, HMPPS does have victim liaison post sentence, the Probation Service's Victim Contact Scheme ('VCS'). The VCS, in various forms, has been operational since 2001, and it is available to individuals who are victims of violent, sexual or terrorism offences where the offender is sentenced to 12 months' imprisonment, or more. Contact in relation to potential data breaches or ongoing police investigations is not within its remit.

94. Where the victim chooses to receive services provided under VCS, they are assigned a Victim Liaison Officer ('VLO'), employed by the Probation Service, who will provide information considered appropriate in all circumstances of the case, which can include updates about the offender's sentence, release, parole review (where applicable), or when they move to open conditions. When it comes to an offender's parole review, the VCS offers victims the right to make representations to the Parole Board about conditions of release and opportunity to submit a victim personal statement explaining the ongoing impact of the offence on them. The VCS is a statutory scheme underpinned by the Domestic Violence, Crime and Victims Act 2004 (the 'DVCVA'), which sets out the eligibility requirements and the information which can be shared.

95. Whilst it would have been possible to reach out to the Family Liaison Officers for them to notify the bereaved families and those VC was charged with attempting to murder, regarding the inappropriate access to case files, such action would have been outside of the legal basis of the VCS.

96. In December 2024, SEROCU notified HMCTS in advance of writing to the bereaved families and subsequently confirmed that they had informed the families that the Unit was investigating alleged data breaches by a former HMCTS employee and current HMPPS employees. The other two HMCTS staff under investigation by the police were not mentioned in the SEROCU letter.

97. After the letter had been sent by SEROCU, the MoJ press office (which also handles press enquiries on behalf of HMCTS and HMPPS) received a press enquiry from a journalist who had apparently seen the letter from the police. Whilst the MoJ did not comment on the investigation, it was confirmed to the journalist that a member of HMCTS staff mentioned in the letter was no longer employed by HMCTS, which was correct at the time of that press enquiry.

98. In March 2025, the MoJ press office received a press enquiry from a journalist asking for confirmation that two named members of HMCTS staff had been dismissed for allegedly accessing information without authorisation. Whilst the

MoJ did not comment on the police investigation or the employment record of any individual, it was confirmed to the journalist that following an internal HMCTS investigation, two further individuals involved in the incident (in addition to the one that was confirmed in response to the December press enquiry) were now no longer employed by HMCTS.

99. In relation to unauthorised access to court records by HMCTS and HMPPS staff, the Minister communicated with the bereaved families on the following occasions: 23 December 2024, 7 April 2025, and 15 April 2025. In response to an enquiry from the bereaved families' solicitor, the HMCTS CEO wrote to a litigation executive at Hudgell Solicitors in May 2025. They were unable to answer all the questions posed by the solicitors, as to do so may have prejudiced the police investigation, but confirmed a number of important points and offered to meet with the families, once all relevant proceedings had concluded.

100. Parliamentary Under-Secretary of State, Alex Davies-Jones MP, has been in contact with surviving victims' and bereaved families, discussing ,matters such as the launching of the Nottingham Inquiry and specific points of contact across Government on this case.

IMPROVEMENTS SINCE THESE EVENTS

101. A number of steps have been taken since these events were discovered and improvements continue to be made.

102. On June 2024, HMCTS provided written submissions to the Minister of State for Courts and Legal Services, Sarah Sackman KC MP, regarding measures in place to manage DCS user access **[WITN0065021]**. The submission detailed a recommendation on whether a commitment should be made to provide external parties, such as families, proactive information in cases of unauthorised access. The recommendation to the Minister was to note the current and planned measures in place to manage the appropriate user access to DCS, and to agree

that in cases where internal investigations and/or police investigations are initiated, that the department adopt a case-by-case approach to managing communications with external parties such as families.

103. HMCTS has progressed/is progressing work to improve guidance for staff users, including:

103.1. Improvements to intranet guidance pages to make it easier for staff to locate and identify relevant guidance;

103.2. Issuing a reminder and re-circulating internal user guidance, with amendments to ensure it reflects current DCS functionality **[WITN0065022]**; and,

103.3. Work to update and strengthen the invitation only DCS functionality Job Card, so as to increase the use of the 'invite only' functionality to restrict case access and ensure the appropriate escalation path is documented (for example, by including improved examples of when the functionality should be used). This will be followed up with associated training on when access restrictions should be applied and how to apply restrictions effectively.

104. HMCTS is also reviewing current assurance checks to evaluate the effectiveness of existing controls and identify areas for improvement in monitoring and enforcement. In addition, HMCTS has instructed a senior civil servant in the organisation to lead a review of all HMCTS policies and procedures relating to unauthorised access, and to convene a cross HMCTS task and finish group comprising all interested parties with a view to making a series of improvement recommendations. Recommendations for improvement are sought on areas including training, communications, guidance, assurance, digital & technology, and access for all HMCTS digital case management systems used by HMCTS staff.

105. In April 2025, the HMCTS SIRO also issued an all-staff communication on the HMCTS intranet, reminding staff of their information security responsibilities and the consequences of inappropriately accessing information **[WITN0065023]**. Alongside the communication, a new policy was issued on 'Inappropriate Access of Case Information on Digital Systems' **[WITN0065024]**.

106. At the relevant time, there was no additional bespoke guidance provided to EMPS around DCS access controls. Guidance in relation to accessing digital systems is now provided in the Probation Court Services Policy Framework implemented on 6 January 2025.

107. A guidance document, titled 'Court Applications Guide' has also issued to EMPS staff which gives an overview of the different systems used by Probation Service staff working in a court role. The guidance also provides important information regarding access as follows: *"As with all the applications we use, we have a responsibility to only access the information we require in our probation roles. Anything we view or download will be visible to the owners of the applications. The consequences of abusing our access rights will be serious"*.

108. In relation to DCS, the guidance gives a clear instruction to access the training platform before a request to the live system is made, and it clearly states that unauthorised access is a criminal offence under the Computer Misuse Act 1990. An email was sent by the Head of Service on 8 July 2025 to the EMPS Strategic Court Leads, for them to disseminate the guidance to their probation staff in the East Midlands region; distribution and adherence to this guidance document will be monitored via the regional courts board **[WITN0065025 ; WITN0065026].**

109. HMPPS is working closely with HMCTS to ensure that probation users are limited to those who have a legitimate business need to use the system and that terms and conditions of use are clear to those users. For probation purposes, HMPPS has agreed with HMCTS that the legitimate business need is limited to individuals whose roles include a daily or routine function to assist or support the

court in decision making or administration. HMPPS has worked with probation regions to refresh the list of probation Access Co-Ordinators roles and ensure they are limited to SPOs and Senior Administrative Officers (SAOs) working in court teams. Those staff will act as the final arbiter in either accepting or rejecting all new requests for a DCS account by probation staff to the cases listed at their local Crown Court centre. They will also be responsible for running regular reports to ensure only those staff who continue to be eligible for a legitimate DCS account have one. They will be supported by having an escalation route to a Single Point of Contact (SPOC) in the Probation Operations Directorate within HMPPS headquarters, for any cases where a decision on access cannot be resolved regionally. In turn, that SPOC role in HMPPS headquarters will liaise regularly with HMCTS staff responsible for the DCS system to ensure that HMPPS is adhering to the requirements for probation usage of the system. These roles and processes will be reinforced by a Memorandum of Understanding between HMPPS and HMCTS, which is being finalised. The HMPPS policy framework document "PI 34 2014 – Conduct and discipline" has been updated **[WITN0065027]**.

110. It is the view of senior operational management in HMCTS that no changes are required to the way video and audio evidence is managed in high-profile cases. The additional access restrictions provided by the existing split between the DCS and DEMS systems provides an appropriate framework for protecting the integrity of sensitive multimedia evidence.

FURTHER MATTERS TO ASSIST THE INQUIRY

111. The independent review commissioned by the Permanent Secretary on 20 January 2025, into the efficacy and interoperability of relevant polices 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') concluded that the guidance for staff in relation to disciplinary action was not aligned within the agencies **[WITN0065028]**.

112. This led to inconsistent approaches between agencies, when dealing with issues of the same nature. The Review set a recommendation for harmonisation of the conduct policies with one overarching policy implemented, to ensure consistency an approach across the Department. Work is underway to implement this recommendation.

113. This Review assessed the policies and procedures, escalation processes, and communication processes between the MoJ HQ and its executive agencies; HMCTS and HMPPS. The purpose of the review was to ensure that the MoJ had appropriate policies and processes in place when handling matters when there is an allegation or suspicion of potential illegal activity on the part of employees or contractors.

114. The review focused on the following general issues:

114.1. Are there formal escalation processes in place in each organisation and with clear escalation routes to MoJ?

114.2. Are thresholds for escalation clearly defined, including to whom, and do those thresholds match the MoJ departmental risk appetite?

114.3. In general, are colleagues aware of the escalation processes?

115. A short questionnaire was issued to staff in HMCTS and HMPPS, to assess general awareness and application of policies. The survey concluded that 96% of staff knew how to report and escalate incidents with 65% being confident in reporting fraudulent activity. In relation to reporting misconduct 90% of staff followed the correct process for reporting.

116. A report was prepared which provided an assessment of the issues and concluded that the policies provided clear definitions and reporting process for

MoJ staff. They did, however, lack adequate communication protocols for high profile or high impact incidents.

117. The report also concluded that the guidance for staff in relation to disciplinary action was not aligned within the agencies. This could lead to inconsistent approaches between agencies when dealing with issues of the same nature.

118. The Review made 14 recommendations for improvement, with a priority rating set against each one. These recommendations included requirements to update and align policies and procedures across the MoJ. Requirements were set to ensure alignment for escalation to senior staff members and teams within the MoJ HQ and its executive agencies.

119. Each of the recommendations was assigned to an 'SCS2' Director, a senior leadership position within the Senior Civil Service, to oversee their completion 12 recommendations have been completed and two remain open, which are due to be completed by April 2026.

120. Work is underway to have a single Code of Conduct and a single Disciplinary Policy for the whole of the MoJ. Consistency and harmonisation of policy forms part of this policy review, but also wider alignment to the recommendations made by Jennifer Rademaker , in her review of HMPPS Professional Standards (published on 6 May 2025) and a cross-government programme called Synergy, which is intended to provide consistent and easily accessible policies across the MoJ, the Home Office, the Department for Environmental, Food and Rural Affairs, and the Department for Work and Pensions. The new policies are expected to be delivered by April 2026.

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: 06/11/2025

INDEX TO FIRST WITNESS STATEMENT OF AMY HOLMES

No.	URN	Document Description
1.	WITN0065002	Where to add documents in the Digital Case System for trial and committal for sentence cases
2.	WITN0065003	Where to add documents in the Digital Case System for probation breach cases
3.	WITN0065004	Annex – DCS Lifecycle Overview
4.	WITN0065005	DCS Screenshot – T&Cs.
5.	WITN0065006	DCS Screenshot – case access justification prompt
6.	WITN0065007	2019 HMCT Counter Fraud, Bribery & Corruption Policy and Response Plan.docx
7.	WITN0065008	2025 HMCT Counter Fraud, Bribery & Corruption Policy and Response Plan.docx
8.	WITN0065009	Annex - Current DCS Intranet Page - About Us Tab.pdf
9.	WITN0065010	Annex - Current DCS Intranet Page - About Us Tab.pdf
10.	WITN0065011	Annex - Current DCS Intranet Page – Training Tab.pdf
11.	WITN0065012	Digital case system dcs-kccs
12.	WITN0065013	Crown Court Digital Case System guidance: register and access case material - GOV.UK
13.	WITN0065014	Crown Court Digital Case System guidance: register and access case material - GOV.UK
14.	WITN0065015	invitation-only-job-card
15.	WITN0065016	CRI031 Limited Access Offenders v2.1
16.	WITN0065017	PI-34-2014-Conduct-and-Discipline.doc
17.	WITN0065018	NPS CD Guidance final v1 -2019.doc
18.	WITN0065019	MoJ discipline-policy-and-guidance
19.	WITN0065020	MoJ Data Protection

20.	**WITN0065021**	130625 HMCTS submission on DCS (final).docx].
21.	**WITN0065022**	Need to know_ issue 26 (July 2025 Online Guidance
22.	**WITN0065023**	Inappropriate access of case information Communication Text April 2025.docx
23.	**WITN0065024**	Inappropriate access of case information Communication Text April 2025.docx
24.	**WITN0065025**	FW Guidance for using HMCTS systems HMPPS with email chain
25.	**WITN0065026**	Attachment to WITN0065025: Court Applications Guide - Guidance for using HMCTS Systems
26.	**WITN0065027**	PI 34-2014 – Conduct and discipline Feb 2025 update.doc.
27.	**WITN0065028**	Independent Review of HMCTS, HMPPS and MoJ policies