

THE NOTTINGHAM INQUIRY

CLOSING STATEMENT ON BEHALF OF THE MINISTRY OF JUSTICE

Introduction

1. These written submissions are made on behalf of the Ministry of Justice (MoJ) and its Executive Agencies, His Majesty's Courts and Tribunal Service (HMCTS) and His Majesty's Prison and Probation Service (HMPPS).
2. The MoJ has sought to assist the Inquiry by providing evidence and documentation, making witnesses available and commissioning and implementing internal reviews. That approach reflects its commitment to transparency, accountability and learning.
3. Whilst the role of the MoJ has been to assist the Inquiry with its essential work in relation to the unauthorised access by HMCTS and HMPPS staff to confidential and sensitive material in this case, it has nonetheless maintained a presence at the Inquiry throughout and has listened carefully to the evidence in its entirety. This has enabled the MoJ to hear and understand all the evidence in its proper context and to better understand the position taken by all those impacted by the events on and after 13 June 2023. The attention that the MoJ has given this Inquiry enables it to assist the Chair to the fullest extent.
4. The pain and loss suffered by the bereaved and survivors is unimaginable. To the family and friends of Barnaby Webber, Grace O'Malley-Kumar and Ian Coates and to Wayne Birkett, Sharon Miller and Marcin Gawronski, the MoJ want to express, again, their condolences and sympathies to you. They also want to repeat what was said by Amy Holmes in evidence - they are sorry¹. The MoJ is sorry for any part it had to play in exacerbating the pain and sorrow suffered by all in this case.

¹ Evidence of Amy Holmes [INQT0000049], 14 April 2026 (AM), 96/3.

5. The MoJ has always appreciated and continues to appreciate the significance of the unauthorised access of records to all those impacted and to society in general. This is a serious matter. There has been no and there will be no minimisation of what happened. There was clear and admitted unauthorised access. The MoJ has reviewed the circumstances of the incident and are continuing to make improvements to processes to reduce the risk of similar incidents occurring in the future. As stated at the very outset of this Inquiry, the MoJ welcomes any recommendations that may be forthcoming should the Chair feel that more can be done.
6. Communication with those at the heart of this Inquiry has been a central theme throughout the course of the evidence. The MoJ and its Executive Agencies accept that in this very sensitive case, they could and should have communicated better with the bereaved families and survivors. The approach to such communication is and will continue to be better in the future.

Structure of these submissions

7. These submissions will focus predominantly on the unauthorised access to sensitive material within the Digital Case System (DCS). However, the MoJ will also seek to assist the Chair with some observations on ancillary matters that have been raised during the course of the evidence and about which the MoJ may be able to assist.
8. These closing submissions are structured as follows and will be presented in two parts.
9. Part 1 will cover the unauthorised access in the following way:
 - 9.1. The Crown Court Digital Case System (DCS) operating procedures
 - 9.2. What the evidence establishes about the nature and extent of the unauthorised access
 - 9.3. The circumstances within which the unauthorised access occurred
 - 9.4. The underlying cause of the unauthorised access
 - 9.5. The adequacy of response to the unauthorised access

- 9.6. Impact and harm
- 9.7. Improvements and changes made
- 9.8. Further learning
- 10. Part 2 will contain some brief observations on two ancillary matters that have featured in the evidence:
 - 10.1. The experience of those navigating the Criminal Justice System
 - 10.2. The work of the Mental Health Review Tribunal.

PART 1: The Crown Court Digital Case System (DCS) operating procedures

- 11. As explained by Amy Holmes, Interim Director General for the Chief Operating Officer Group, in her witness statement and in her oral evidence, the Courts and Tribunals Service uses a system known as DCS, which stands for Digital Case System. It is an electronic system used predominantly in the Crown Court for the storage of case files and documentary evidence in a criminal case².
- 12. The system enables multiple individuals to upload and access case information. Those individuals include members of the judiciary, parties involved in the case, and other Criminal Justice System (CJS) partner agencies such as the Crown Prosecution Service (CPS) and HMPPS. The DCS system will be initially set up when a case is sent / committed to the Crown Court and will remain active for the management and conduct of any appeals. This is set out in the underlying policy document setting out the DCS lifecycle overview³.
- 13. The evidence provided in this inquiry shows that there was a system in place at the time of these events to oversee controlled and appropriate access to material held on the DCS and systems in place for responding to any issues related to its use⁴. That system may be summarised as follows:

² Evidence of Amy Holmes [INQT0000049], 14th April 2026 (AM), 79/1–80/13; 1st Statement of Amy Holmes [WITN0065001] at para. 13–25.

³ Policy Document, Re: The Workflow Interactions and DCS Lifecycle Overview, HMCTS [WITN0065004].

⁴ 1st Statement of Amy Holmes [WITN0065001] at para. 18, 19, 20.

- 13.1. For all new users of DCS in roles that can access cases without invitation, a controlled registration process exists before access is granted and this is scrutinised and approved by Access Co-ordinators for the role.
- 13.2. Access can only be linked to an email account with a domain recognised by DCS.
- 13.3. Once an account is set up there are mandatory online Terms and Conditions that must be signed by all system users.
- 13.4. The first term that must be agreed sets out the litmus test for access: *'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'*. There are other terms of relevance before use, including, a requirement to comply with the Data Protection Act 2018⁵.
- 13.5. HMCTS Guidance on the DCS⁶ defined business need as being required to 'complete an activity on DCS or to use information stored on DCS to assist in carrying out duties'. This was accompanied with guidance on appropriate use.
- 13.6. A further prompt sits within the system when a user seeks to access a case outside of their own assigned geographical work location. It is an inherent part of the efficient functioning of the criminal justice system that cases may need to be managed by or between different court areas geographically. The reasons for this are explained in the statement of Amy Holmes⁷. When a user attempts to access a case outside of their assigned work location the system generates a further prompt that requires them to enter the business need and reason for their access⁸. This part of the system is audited, as set out in more detail below. In her oral evidence, Amy Holmes stated that any information entered regarding the need to

⁵ Policy Document, Re: Terms & Conditions (including Acceptable Use) for the Crown Court Digital Case System (DCS) [WITN0065005].

⁶ Policy Document, Re: Crown Court Digital Case System - About us, HMCTS [WITN0065009].

⁷ 1st Statement of Amy Holmes [WITN0065001] at para. 26–30.

⁸ Crown Court Digital Case System, Case Outside Working Area [WITN0065006].

access a case outside of one's location is audited through reports run regularly.⁹

- 13.7. The DCS system contains a number of role-based access controls. Examples of this include a private section for the judiciary and HMCTS staff only and a section for unused prosecution material, which is not visible to HMCTS Staff, Probation Staff or Judiciary.¹⁰
- 13.8. For cases of special sensitivity, the system allowed for restricted access by using an 'invite only' functionality, introduced on 10 May 2021. At the relevant time this functionality could be used for high profile cases, cases with high levels of media interest or where a member of the criminal justice system is personally involved in the cases. Changing from or to the 'invite only' functionality could be done at any time and could be applied for limited periods only¹¹. This part of the system was supported with a Job Card explaining the use of this functionality with a detailed flowchart of the process¹². This included clear guidance on the way in which an 'invite only' notification may be implemented and by who.
- 13.9. Procedures were in place for those no longer working in roles requiring access to DCS such that managers were responsible for a leavers checklist which included a requirement for the staff member to be removed from DCS system access¹³.
- 13.10. Training and guidance were in place for all DCS users. Significant user guidance was available as well as Job Cards and key control checks, setting out a number of processes and compliance checks. A number of those available since 31 July 2019 have been provided to the inquiry and were outlined in the witness statement of Amy Holmes¹⁴. In her evidence at the inquiry, Amy Holmes confirmed that access based on a legitimate business need formed part of the training provided to users of DCS¹⁵.

⁹ Evidence of Amy Holmes [INQT0000049], 14th April 2026 (AM), 82/12–20.

¹⁰ Evidence of Amy Holmes [INQT0000049], 14th April 2026 (AM), 79/24–80/9.

¹¹ Policy Document, Re: Crown Court Digital Case System - About us, HMCTS [WITN0065009].

¹² Job Card: Invitation Only DCS Functionality, V2 July 2021, HMCTS [WITN0065015].

¹³ Policy Document, Re: Leavers Checklist for Managers, MoJ [WITN0065014].

¹⁴ 1st Statement of Amy Holmes [WITN0065001] at para. 22–23; HMCTS User Guidance [WITN0065009], [WITN0065010], [WITN0065011], [WITN0065013]; Job Cards & Key Control Checks [WITN0065012], [WITN0065015].

¹⁵ Evidence of Amy Holmes [INQT0000049], 14th April 2026 (PM), 4/17–5/2.

Additionally, annual training was in place for all HMPPS and HMCTS staff on 'Security and Data Protection Fundamentals', which included training on data types and protection principles. All internship staff were subject to the same training requirements as permanent members of staff.

- 13.11. A number of systems were in place to monitor and oversee operational use of the DCS. Importantly the role of Access Co-ordinator was in place. In addition to providing the safeguard of approving initial access to the DCS, the Access Co-ordinator within HMCTS was responsible for monitoring access to DCS by way of monthly 'user count' and 'user location v case location' reports. These two safeguards enabled HMCTS to monitor and audit DCS access and in turn to identify any potential unauthorised access. Additionally, the ability to view the Record of Case Activity (RoCA) was open to all DCS users who can access a RoCA tab on the system for spot-checking at any time¹⁶. Access Co-ordinators were also automatically invited to 'invitation only' cases to enable checks to be carried out. Furthermore, local management was responsible for removing access upon a member of staff leaving.

14. At the relevant time, each of the Executive Agencies involved in this case operated their own separate and admittedly differing procedures to deal with any alleged unauthorised access to data. Within HMPPS, a policy framework document 'PI 34 2014 – Conduct and Discipline' governed investigations into any alleged unauthorised access to data¹⁷. The instruction provides a wide range of options for dealing with staff who fail to meet the required standards of behaviour and covers investigations into staff misconduct and discipline. The National Probation Service (NPS) Conduct and Discipline Guidance (October 2019)¹⁸ also applied to support the consistent application of the said Conduct and Discipline Policy. Within HMCTS the Counter Fraud Policy and Response Plan applied where staff were found to have accessed material without a business need to do so and accordingly disciplinary action would be taken with an invitation to the

¹⁶ Evidence of Amy Holmes [INQT0000049], 14th April 2026 (AM), 85/12–86/24; 1st Statement of Amy Holmes [WITN0065001] at para. 20, 21, 30; Policy Documents re: auditing processes [WITN0065006], [WITN0065007], [WITN0065008].

¹⁷ Policy Document re: Conduct and Discipline, National Offender Management Service [WITN0065017].

¹⁸ Policy Document, Re: NPS Conduct and Discipline Guidance, HMPPS [WITN0065018].

police to investigate¹⁹. HMCTS also followed the MoJ Conduct Policy and Discipline Policy and Guidance²⁰.

- 14.1. The MoJ has a Data Protection Team (DPT) which drives the Department's data protection strategy and provides training and advice / support. Within the DPT sits the Data Protection Officer (DPO) who is responsible for reporting any personal data breaches to the Information Commissioner's Office (ICO) and for advising business areas to notify data subjects if the threshold for notification has been reached.
15. The Chair is invited to view this wide systemic framework within an even broader context which recognises the overarching need for HMCTS to administer and support the work of the criminal courts in a manner that requires considerable flexibility and in a way that optimises efficiency and necessarily entails a level of access to digital systems across different teams and / or sites. As Amy Holmes explained in her statement²¹, intra and cross court access is a regular and essential part of case management and administration. There is a balance to be struck. The tighter the access controls in place, the more strain might be put on the efficiency of the service. The system that existed at the time sought to provide a balance between ease and efficiency of accessibility and the protection of data.

The nature and extent of the unauthorised access

16. Notwithstanding the systemic safeguards in place, the evidence in this case establishes that individuals within both HMCTS and HMPPS accessed VC's case files on DCS without a legitimate business need to do so. The evidence in this regard is not contested, and the Chair will undoubtedly find:

- 16.1. HMPPS:

- 16.1.1. On 25 January 2024 a RoCA report identified access to VC's case files on DCS where there may not have been a business need for such access

¹⁹ Policy Document Re: Counter Fraud, Bribery & Corruption Policy and Response Plan, HMCTS [WITN0065007] at page 14; Report [WITN0065008] at page 4, 18–19.

²⁰ Policy Document re: Human Resources Directorate: Discipline policy and guidance, September 2017, Ministry of Justice [WITN0065019].

²¹ 1st Statement of Amy Holmes [WITN0065001] at para. 28.

- 16.1.2. On 29 January 2024 information was provided to East Midlands Probation Service (EMPS). At that time, it was felt that 11 members of probation staff may have accessed the DCS illegitimately.
- 16.1.3. On 30 January 2024 an HMCTS Delivery Manager reported the identified incidents to the HMCTS Data Incidents Team who referred the matter to the HMCTS Counter Fraud Team.
- 16.1.4. Four members of the 11 initial members of staff were quickly identified as having a legitimate business need to access VC's DCS.
- 16.1.5. Seven members required further investigation. This consisted of four case administrators and three probation service officers. As set out in paragraph 64 of Amy Holmes' statement²², that access occurred by three members of staff between 19 and 26 June 2023, so shortly after the case was uploaded to DCS and by four members of staff between 20 and 26 January 2024, at or around the time of VC's sentencing hearing.
- 16.1.6. HMPPS determined from their own further investigations that access by the four case administrators was acceptable and in accordance with their expected roles. No further action was taken by HMPPS against them. In respect of the three probation officers, it was determined that whilst each did not have a clear need to access the case, their actions would not trigger a further conduct and disciplinary investigation, and they were issued formal improvement actions. The rationale for this is explained by Amy Holmes in her statement²³ and relates to the members of staff being relatively new in post and still within their training periods. Each individual was subjected to a conversation with the East Midlands Counter Corruption Lead, and all probation staff underwent a Counter Corruption briefing at Nottingham Crown Court.

²² 1st Statement of Amy Holmes [WITN0065001] at para. 64.

²³ 1st Statement of Amy Holmes [WITN0065001] at para. 65.

- 16.1.7. The HMCTS Counter Fraud Team's investigation of HMPPS staff commenced on 1 February 2024. On 14 May 2024 the HMCTS Chief Information Security Officer informed the Senior Information Risk Owner in HMCTS of the intention to refer the aforesaid seven members of staff to the police for investigation.
- 16.1.8. On 21 May 2024 referrals to Nottinghamshire Police were made in respect of HMPPS staff access. On 9 June 2024 Nottinghamshire Police informed HMPPS that they were not intending to investigate the matter further.
- 16.1.9. HMPPS next heard from SEROCU (South East Regional Organised Crime Unit) in early December 2024 that they would be investigating these matters further.
- 16.1.10. On 26 June 2026 the MoJ were informed that SEROCU had concluded their investigation and that no further action was being taken by them.
- 16.2. HMCTS:
- 16.2.1. As part of the HMCTS Counter Fraud Team investigation into HMPPS, a number of audit logs of DCS access were reviewed and on 16 May 2024 the Counter Fraud Team commenced investigation into possible unauthorised access to DCS records by HMCTS staff.
- 16.2.2. The MoJ accept that prior to Amy Holmes giving evidence there was a need to clarify the initial information provided to the Inquiry regarding the number of HMCTS staff who had accessed VC's case without a business need to do so. Amy Holmes' first statement had covered three members of HMCTS staff who had accessed DCS but did not reference an individual who was undertaking an internship and was a fourth member of HMCTS staff to have accessed VC's case without a business need to do so. The omission of this information in the first statement is regrettable and the MoJ apologises for this. As soon as this omission came to light immediate steps were taken to ensure that the fullest corrected information was

provided to the inquiry by way of a supplemental statement from Amy Holmes²⁴.

- 16.2.3. The totality of the evidence that is now before the inquiry is that four members of HMCTS staff accessed the case without a business need to do so. This included two full-time members of Nottingham Crown Court staff who accessed the case between 18 and 23 January 2024 and an intern who was employed by HMCTS as an Administration Officer, via a summer placement scheme, between 3 July and 25 September 2023, and who accessed information without a business need to do so on 21 September 2023. The fourth member of staff was identified to have accessed the case from Lewes Crown Court on 19 June 2023.
- 16.2.4. HMCTS liaised with Nottinghamshire Police concerning their conclusions about not investigating matters further and as conveyed to HMPPS on 9 June 2024.
- 16.2.5. In August 2024 HMCTS submitted evidence to Nottinghamshire Police. On 3 October 2024 they were told that an officer had been assigned to the case. In October 2024 further files of evidence were provided by HMCTS to SEROCU and Sussex Police. On 8 November 2024 the HMCTS Counter Fraud Team shared an evidential file with the police. The supplemental statement of Amy Holmes provides more detail to the inquiry as to the delayed reporting of the fourth member of HMCTS staff to the police. Although that member of staff's details was contained within documents sent to the police as early as 25 July 2024, a direct referral to the police regarding this fourth member of staff was not made until December 2024. Again, the MoJ apologises for this²⁵.
- 16.2.6. On 26 June 2026 the MoJ was informed that SEROCU have concluded their investigation and that no further action is being

²⁴ 2nd Statement of Amy Holmes [WITN0065029] at para. 3–15.

²⁵ 2nd Statement of Amy Holmes [WITN0065029] at para. 1–15.

taken by them. The MoJ have not received any further update in respect of any investigation by Sussex Police.

16.2.7. In addition, HMCTS instigated disciplinary action against the two permanent members of Nottingham Crown Court staff resulting in their dismissal and no longer being in the employment of HMCTS. The member of staff from Lewes Crown Court resigned when the unauthorised access was identified.

17. It is fully acknowledged that where any police investigations remain ongoing, nothing in these submissions should risk prejudicing those investigations. It is however accepted that four members of HMCTS staff and three probation service officers employed by HMPPS have been shown through internal investigations to have accessed DCS without a business need to do so.

The circumstances within which unauthorised access occurred

18. The MoJ does not seek to justify the identified unauthorised access in any way. It should not have happened and the MoJ and its Executive Agencies repeat their apologies in this regard. Amy Holmes was asked whether there was 'needless voyeurism' by those who accessed material with no business need to do so. It is not known what the motivation of the relevant individuals at HMCTS and HMPPS was, but Ms Holmes accepted that this could be a legitimate description of what happened²⁶.

19. However, when the Chair considers the unauthorised access the MoJ would wish to make five important points relevant to the overall circumstances and context:

19.1. The method by which the unauthorised access was uncovered was the existing internal auditing system in place. This shows there was an effective auditing system in place at the relevant time that was able to identify who had accessed DCS, when it was accessed and what was accessed²⁷. Amy Holmes also confirmed in evidence to Mr Moloney KC that there had been a full audit of all access to relevant documents by MoJ employees across the East Midlands HMCTS region²⁸.

²⁶ Evidence of Amy Holmes [INQT0000050], 14th April 2026 (PM), 9/6-16.

²⁷ Evidence of Amy Holmes [INQT0000050], 14th April 2026 (PM), 5/3-13.

²⁸ Evidence of Amy Holmes [INQT0000050], 14th April 2026 (PM), 1/5-12.

- 19.2. There is no evidence that any member of staff ever viewed – or were able to view - any moving images, footage or CCTV of the incident. The way in which DCS works means that moving images are not stored and they are not accessible through this platform. Amy Holmes confirmed in her oral evidence that DCS cannot hold any type of digital footage or audio recordings²⁹. This point is not intended to minimise what did happen but to offer some reassurance to the bereaved and the survivors in this small regard.
- 19.3. There is no evidence that the MoJ are aware of to date that suggests any downloading by any individual of material accessed on DCS.
- 19.4. There is no evidence that the MoJ are aware of to date that suggests any sharing by any individual of material accessed on DCS³⁰.
- 19.5. The evidence supports the contention that the unauthorised access in this case was by a low number of individuals. The evidence at the inquiry was that around 2000 court staff at HMCTS and just over 2000 HMPPS court staff have access to DCS³¹.

The underlying cause of the unauthorised access

20. The MoJ accepts that unauthorised access to material on DCS may constitute serious misconduct. At the same time, the evidence in this inquiry supports the position that such conduct was not routine, encouraged, or tolerated and it arose within a framework where access was governed by policy and training.
21. Within those frameworks two underlying causes for the unauthorised access may be identified:
- 21.1. A failure to utilise available safeguards by not applying the 'invite-only' restriction that was available: HMCTS accepts that it should have been applied earlier in this case³². Had it been applied then it is arguable that

²⁹ Evidence of Amy Holmes [INQT0000050], 14th April 2026 (PM), 6/2-11.

³⁰ Evidence of Amy Holmes [INQT0000050], 14th April 2026 (PM), 6/12-18.

³¹ Evidence of Amy Holmes [INQT0000049], 14th April 2026 (AM), 79/13-23.

³² Evidence of Amy Holmes [INQT0000049], 14th April 2026 (AM), 83/23–84/7.

the access in question may not have happened. It is also accepted that its application in May 2025 was also later than it should have been, given the issues which had already long been identified. However, there is no evidence that any further unauthorised access occurred at any time after January 2024.

- 21.2. Operational errors by individuals: staff were trained, instructed and bound by terms and conditions setting out the rationale for accessing material on DCS. However, no system is infallible and clearly the members of staff concerned acted outside of their training and instruction. The Chair explored whether this was 'needless voyeurism' by members of staff. The MoJ, and its corporate witness Amy Holmes, cannot discount this potential cause. There may be other causes such as misplaced professional curiosity. However, the MoJ offer no justification for any unauthorised access, whatever the cause, and Amy Holmes accepted in her evidence that the access was not accidental in any way³³.

Adequacy of organisational response to the unauthorised access

22. It is submitted that there are three important angles to consider here:

- 22.1. The internal organisational responses
- 22.2. The threshold for reporting to the ICO
- 22.3. Communication with those impacted by the unauthorised access

Internal organisational responses

23. It is acknowledged that the two Executive Agencies responded in different ways to the unauthorised access identified within their own organisations. The evidence before the Inquiry shows a degree of institutional fragmentation with inconsistent responses across MoJ bodies. This led to differing approaches to discipline, differing thresholds for escalation and parallel processes operating without sufficient coordination. It is feasible that the relative infrequency of this issue arising led to such fragmentation. Furthermore, as Amy Holmes explained in her oral evidence, there was collaboration between HMCTS and HMPPS, but various

³³ Evidence of Amy Holmes [INQT0000049], 14th April 2026 (AM), 88/19-24.

investigations were taking place³⁴ and it is accepted that there was, arguably, insufficient alignment of governance and escalation frameworks at the time.

Threshold for reporting to the ICO

24. With respect to the approach to formal reporting of personal data breaches under data protection law, this is more complex. A number of general points may assist:

- 24.1. Paul Arnold³⁵ explained in his evidence, albeit in relation to a question about unlawful access to medical records, that where an incident occurs within an employment setting then the position of the ICO is that the employer is expected to conduct their own workplace investigation to confirm and determine what happened and then, if a referral is necessary, it will be considered by the ICO at that point³⁶.
- 24.2. He also confirmed that records pertaining to a deceased person are outside of the protection of the Data Protection Act 2018 but personal information about family members and any survivors would be within the scope of the protection of data protection legal framework³⁷. Other legislative provisions may be of relevance for investigations by other authorities, for example, the police.
- 24.3. In the UK, personal data processing is governed by the UK General Data Protection Regulation (the Regulation) and the Data Protection Act 2018 (the Act). Part 3 of the Act 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 high risk to the rights and freedoms' of the data subject.
- 24.4. When the MoJ's DPT are made aware of a personal data incident there will be an initial assessment. If the outcome of the assessment is that the incident is high / substantial in severity, then it is escalated to a senior member of the DPT who will convene an incident review panel.

³⁴ Evidence of Amy Holmes [INQT0000049], 14th April 2026 (AM), 93/16–94/2.

³⁵ Interim Chief Executive and Deputy Commissioner of the Information Commissioner's Office.

³⁶ Evidence of Paul Arnold [INQT0000095], 26th May 2026 (AM), 31/2-18.

³⁷ Evidence of Paul Arnold [INQT0000095], 26th May 2026 (AM), 31/19–32/5.

- 24.5. The incident review panel consists of senior operatives including the Data Protection Officer, a Deputy Data Protection Officer, and a Data Protection Strategic Lead. The panel will assess whether the threshold for notification to the ICO or data subjects has been reached.
25. On 29 January 2024 a Senior Probation Officer informed the MoJ DPT about the unauthorised access to records. On 30 January 2024 further information was sought from the DPT as set out in the witness statement of Amy Holmes³⁸. That information included whether any data had been downloaded and the extent of any access. Based on the information provided by HMPPS the DPT did not consider that the incident warranted an incident review panel. The MoJ Information Security Team was notified of this.
26. No further action was taken by the DPT at this time. In December 2024 the Executive Agencies became aware, following referral to them, that SEROCU were investigating the case and on 17 December 2024 the CEO of HMCTS and the CEO of HMPPS informed the Permanent Secretary of the unauthorised access. This in turn led to the Permanent Secretary commissioning an independent review into the efficacy and interoperability of relevant policies that had operated in respect of these issues.
27. On 23 April 2025 the DPT convened an incident panel. Following a review of the available information, the panel concluded that although some of the unauthorised access did constitute a data breach, the threshold for reporting to the ICO was not met. The panel also determined that the threshold for reporting to the victims or their families or VC, which is higher than the threshold for reporting to the ICO, was also not met. In reaching this decision, the panel considered a number of mitigating factors. The risk to affected individuals was assessed as low, given the limited nature of the personal data that had been accessed. In addition, a significant proportion of the information was already publicly available through media reporting, reducing the likelihood of any further impact arising from the unauthorised access. The panel also noted that there was no evidence that any information had been extracted, copied, downloaded, shared, or otherwise misused.

³⁸ 1st Statement of Amy Holmes [WITN0065001] at para. 76.

Communication with those impacted by the unauthorised access

28. The inquiry has heard through a combination of the written and oral evidence of Amy Holmes that there were thresholds in place for making contact with those impacted by the unauthorised access³⁹. UK GDPR Article 33 'Notification of a personal data breach to the supervisory authority'⁴⁰ and Article 34 'Communication of a personal data breach to the data subject'⁴¹ applied. These provisions were applied by the MoJ, and this resulted in there being no timely communication of the unauthorised access of records to the bereaved families and survivors at the time the matter came to light. The first contact with the families on this issue was on 23 December 2024 with further contacts in 2025. That contact post-dated the families and survivors becoming aware of these issues through media and police channels.
29. The MoJ does not wish to hide behind the legislative framework, and accepts unequivocally that the bereaved and survivors in this case should have been informed about the unauthorised access to records much sooner. The failure to do this would understandably have compounded the distress already being experienced. This constitutes a failure of candour and victim engagement and the MoJ has listened carefully to what has been said by each and every witness about this issue. In respect of notification to the ICO, the legislation supports the action taken with respect to not notifying the bereaved and survivors of the unauthorised access but as Amy Holmes acknowledged in her oral evidence there is a wider context. The MoJ has updated its Personal Data Incident Management Acceptable Use Protocol and now consideration is given to the wider human

³⁹ Evidence of Amy Holmes [INQT0000049], 14th April 2026 (AM), 96/10-15; Evidence of Amy Holmes [INQT0000050], 14th April 2026 (PM), 1/17-2/1; 1st Statement of Amy Holmes [WITN0065001] at para. 11, 81-83, 88-91.

⁴⁰ Art. 33(1) GDPR "*In the case of a personal data breach, the controller shall [...] notify the personal data breach to the supervisory authority competent [...], unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons [...]*".

⁴¹ Art.34(1) GDPR "*When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay*"; Art.34(3) GDPR "*The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach [...]; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.*"

element underlying a need for greater openness and candour regardless of the law⁴².

30. As the inquiry and indeed those impacted by the unauthorised access have fairly acknowledged in this inquiry, it has not been possible for the MoJ or its Executive Agencies to provide any further information about the nature and extent of the unauthorised access because of the ongoing police investigations and the risk of any prejudice occurring. It is clear from a number of documents that the police have properly been the conduit for further information in respect of their ongoing investigations, which is appropriate in all the circumstances. The MoJ have assisted the police as requested throughout and will continue to do so. The MoJ would however wish to convey in these submissions that when all criminal investigations and / or any actions are concluded, they would be willing to discuss these matters further with those impacted to provide as much further information as may be deemed helpful at that time. It is appreciated that this could be seen as too little too late, but the MoJ makes this offer openly.

Impact and harm

31. The evidence given by all impacted by unauthorised access has been carefully listened to but more importantly it has been heard. The MoJ recognises that it sits as one of a number of organisations whose employees, albeit in lesser numbers, have accessed data that they ought not to have done. It is accepted that this has resulted in additional distress but also a possible loss of confidence in part of the justice system as well as a perception of misuse of position and erosion of trust in how sensitive information is handled.
32. Albeit a small comfort at this time, the MoJ assures this inquiry again, that it is aware of no onward sharing of material viewed on DCS that will have placed any sensitive information from this system into the public domain.
33. The MoJ openly recognises the harm suffered and the importance of restoring confidence and turns now to the improvements and changes made since these incidents.

⁴² Evidence of Amy Holmes [INQT0000050], 14th April 2026 (PM), 7/6-23.

Improvements and changes already made

34. In each area above the MoJ and its Executive Agencies have not sat back and awaited the outcome of this Inquiry nor the police investigations to make improvements. The MoJ has been proactive in identifying and implementing positive change. The work done so far can be summarised as follows:
- 34.1. Improved intranet guidance pages so staff using DCS can identify relevant guidance more easily⁴³.
 - 34.2. In April 2025 the HMCTS Senior Information Risk Owner ("SIRO") issued an all-staff communication on the HMCTS intranet reminding all of their information security responsibilities and the consequences of inappropriately accessing information⁴⁴.
 - 34.3. A new policy was issued on 'Inappropriate Access of Case Information on Digital Systems'⁴⁵.
35. Enhanced guidance for HMPPS on accessing digital systems was provided in the Probation Court Services Policy Framework that was implemented on 6 January 2025. Additionally East Midlands Probation (EMPS) have been reminded in their 'Court Applications Guide' of the importance of only accessing information required for the role being carried out by the service and on 8 July 2025 an email was sent to all EMPS Strategic Leads to disseminate this guidance⁴⁶.
- 35.1. On 2 July 2025 'Need to Know' issue 26 (an internal communications publication) was disseminated to all staff across HMCTS. This included a section on the appropriate use of the DCS, reminding all staff using the system that access is limited to business need only and what this meant⁴⁷. The DCS functionality Job Card has been updated with enhanced guidance as to when this should be utilised. This work forms part of the

⁴³ Policy Documents: internet guidance & training re: DCS [WITN0065005], [WITN0065006], [WITN0065009], [WITN0065010], [WITN0065011].

⁴⁴ Memo from Annabel Burns re: Inappropriate access of case information [WITN0065023].

⁴⁵ Policy Document, re: Inappropriate Access of Case Information on Digital Systems, HMCTS [WITN0065024].

⁴⁶ Email from Sarah Williams to Saika Jabeen re Guidance for using HMCTS systems [WITN0065025]; Policy Document, Re: HMCTS Applications - A Basic Guide for Court Admin [WITN0065026].

⁴⁷ Email from HM Courts and Tribunals Service re: Need to know: issue 26 [WITN0065022].

Task and Finish Group HMCTS has established to develop and implement enhanced access controls within the Digital Case System (DCS). Further information on this work is contained at paragraph 35.6.

35.2. HMPPS and HMCTS have worked closely to ensure Probation Service users are limited to those with a legitimate business need to use the system. This has led to HMPPS having a refreshed list of Access Co-ordinators working within the court teams with responsibilities including the running of regular reports to monitor those who have access to DCS. There are strengthened escalation routes within the service and there is greater liaison with HMCTS to ensure that HMPPS is adhering to requirements. A Memorandum of Understanding between the two Executive Agencies is in development and anticipated to be completed by the end of September 2026 and the HMPPS Policy Framework 'PI 34 2014 has been updated⁴⁸. HMPPS has issued detailed guidance both to probation users of DCS⁴⁹ and to probation service staff carrying out the Access Co-ordinator role⁵⁰. The guidance for probation users of DCS defines what constitutes legitimate use of DCS by probation service staff, sets out user responsibilities for handling case information, explains the controls in place and describes how to report unauthorised access and the consequences for misuse. Copies of these guidance documents have been provided to the Inquiry.

35.3. An Independent Review into the efficacy and interoperability of HMCTS, HMPPS and MoJ policies in high profile, criminal and contentious cases ⁵¹ was commissioned by the Permanent Secretary on 20 January 2025. It concluded that guidance for staff in relation to disciplinary action was not aligned within the Executive Agencies⁵². This lack of alignment could lead to inconsistent approaches when dealing with issues of the same nature. 14 recommendations were made in this review and two of the

⁴⁸ Policy Document re: Conduct and Discipline, National Offender Management Service [WITN0065027].

⁴⁹ Guidance, Re: Crown Court Digital Court System, HM Prison & Probation Service, 1st March 2026 [MOJU0000001].

⁵⁰ Guidance, Re: Crown Court Digital Case Service Probation Local Access Co-Ordinator: Role & Responsibilities, HM Prison & Probation Service, 1st March 2026 [MOJU0000003].

⁵¹ Report dated 04/2025 compiled by Data Protection Team, Ministry of Justice [WITN0065028].

⁵² Report dated 04/2025 compiled by Data Protection Team, Ministry of Justice [WITN0065028] at para. 5.

recommendations remain open relating to the harmonisation of the conduct policy, due to be completed this summer. A senior Civil Service Director has held oversight responsibility to ensure that action has been taken to respond to these recommendations and Amy Holmes confirmed in her oral evidence⁵³ that the guidance is more accessible and much clearer now with a greater emphasis on training and responsibilities as well as clarity on unauthorised access and the consequences arising from that.

- 35.4. Resulting from the review a new process for handling high profile unauthorised access cases has been agreed between HMCTS and the MoJ to avoid inconsistencies in the future.
- 35.5. The MoJ Personal Data Incident Management – Acceptable Use Protocol (AUP) has been updated. This is dated April 2026, and a copy was provided to the Inquiry in May 2026⁵⁴. This aims to strengthen accountability for incident management by clearly defining the role of the DPT and business areas. There is greater oversight, advisory and escalation responsibilities throughout the personal data incident lifecycle.
- 35.6. HMCTS has established the Invite Only Task and Finish Group to develop and implement enhanced access controls within the Digital Case System (DCS). This work includes the introduction of revised and broader access restriction definitions to provide greater clarity to users on when additional access controls should be applied and to ensure that such controls can be used across a wider range of appropriate cases, together with supporting escalation processes and associated system controls. Updated guidance, communications, and training materials are being developed to support the pilot and subsequent implementation of these new arrangements during the final quarter of 2026/27. This work forms part of HMCTS's wider programme of continuous improvement to information management and access controls.

⁵³ Evidence of Amy Holmes [INQT0000049], 14th April 2026 (AM), 106/20–107/4.

⁵⁴ Policy Document, Re: Data Protection Policy Acceptable Use Protocol - Personal Data Incident Management, Ministry of Justice [MOJU0000002].

- 35.7. The HMCTS SIRO has introduced a new Unauthorised Access Improvement Programme. The purpose of the programme is to establish a sustainable organisational framework that enables HMCTS to prevent, detect and respond consistently to unauthorised access to sensitive information, whilst providing confidence to HMCTS Executive Team, the Ministry of Justice and wider stakeholders that data access risks are understood, appropriately managed and subject to effective governance and assurance.
- 35.8. As of July 2026, work on the Code of Conduct and Disciplinary Policy remains a priority. However, policy development has been temporarily paused to allow consultation on the Grievance Resolution Policy to progress. Development will resume once the grievance consultation has reached an appropriate stage. Subject to progress, we are aiming to recommence discussions with the Trade Unions on the Code of Conduct and Disciplinary Policy in the autumn, at which point revised implementation timescales will be confirmed.
36. This work shows that the MoJ has already implemented a series of improvements, including strengthened access controls and system segmentation, enhanced monitoring and audit processes, clearer escalation guidance, revised personal data incident protocols requiring consideration of notifying affected individuals and strengthened training and accountability measures.
37. This marks an important and sustainable enhancement to protective control measures and demonstrates a balanced approach on both technical compliance and human centred considerations.
38. The MoJ accepts that this work must continue. Frameworks were in place, and systems have already been improved, with further improvements in train, which the MoJ hope the Chair will agree offer enhanced and improved protections, systems and responses within what remains a rigid legal framework.
39. The MoJ does not comment on the wider legislative position in respect of data legislation in these submissions and have instead focussed on their own operations within these frameworks.

Further learning

40. As the detailed evidence provided has shown, significant improvements have already been made to reduce the risk of unauthorised access to material held on the DCS. MoJ will continue to work towards making further improvements where this is possible. No specific further recommendations are sought from the Chair but the department and its Executive Agencies will also consider all recommendations made by the Inquiry that are relevant to its operations and management of data.
41. Paul Arnold of the ICO refers to a cultural issue underlying inappropriate data access more generally. Should the Chair consider this issue and any recommendations relating to the underlying risk of unauthorised access to sensitive information, the MoJ respectfully submits that the evidence before the Inquiry demonstrates that, in the instances under consideration, unauthorised access was limited and does not support a conclusion that access to the material in question was widespread beyond those individuals identified through the investigation. That should not, however, be taken to suggest that there is no broader organisational risk to manage. The MoJ recognises that, as with any organisation entrusted with sensitive information, there remains an ongoing risk that individuals may seek to access information without a legitimate business need. For that reason, the MoJ continues to strengthen its preventative controls, monitoring, assurance arrangements and staff awareness. Consistent with Mr Arnold's evidence that there is value in reminding staff of their responsibilities in relation to unauthorised access⁵⁵, the MoJ has already undertaken a number of communications and related assurance activities since these incidents came to light.
42. To the extent the Inquiry considers making recommendations, the MoJ would welcome those that are evidence-based, proportionate to the risks identified and capable of practical implementation across similar bodies, if appropriate. It stands ready to engage constructively with any such recommendations.

⁵⁵ Evidence of Paul Arnold [INQT0000095], 26th May 2026 (AM), 33/12-25.

PART 2: Additional observations on evidence given in the Inquiry

43. The MoJ's engagement with the whole of the inquiry has enabled it to identify two important issues that have featured in the evidence and about which the MoJ seeks to provide some brief comment to assist the Chair in her overall considerations. The first concerns the experiences of those navigating the Criminal Justice System and how they may be better assisted. The second is the role and function of the Mental Health Review Tribunal.

Navigating the Criminal Justice System

44. The MoJ has carefully considered the evidence from all bereaved and survivors, as well as Julian Hendy and Clare Waxman OBE in particular. Since this evidence was given in its totality the MoJ has reflected carefully upon it and wishes to take the opportunity within these submissions to assist the Chair with some observations and updated information in relation to key themes that have emerged.

45. In this section of the submissions the MoJ will consider:

- 45.1. The Victims' Code and Code Compliance
- 45.2. Monitoring of the victim journey / System fragmentation and ownership
- 45.3. Victims Hubs
- 45.4. Advocacy and support provisions

The Victims' Code and Code Compliance

46. The Victims' Code is a statutory Code of Practice, which sets out the services, rights and information that victims can expect to receive from criminal justice agencies in England and Wales. The current Code⁵⁶ was issued under section 32 of the Domestic Violence, Crime and Victims Act 2004 and the new Code, which MoJ recently consulted on, will be issued under section 2 of the Victims and Prisoners Act 2024 (VAP Act) (not yet commenced). The consultation on the new

⁵⁶ Guidance, Code practice for Victims of Crime in England and Wales (Victims' Code) dated 29 January 2025 [HOMF0000067].

Code closed on 30 April 2026. The responses are currently being considered, and a public response will be issued ahead of finalisation of the new Code and before it comes into force.

47. Section 5(1) of the VAP Act (commenced in January 2025) places a duty on service providers under the Victims' Code to comply with the Code unless they have good reason not to. The Code compliance framework in the VAP Act (not yet commenced) includes legislative duties for specified criminal justice bodies to collect prescribed information on Code compliance and share it at a local level. The framework also requires specified criminal justice bodies and 'elected local policing bodies' of a police area at the local level, and Ministers at the national level, to keep under review whether and how services are provided in compliance with the Code. This framework will therefore, for the first time, require local scrutiny and national oversight over specified criminal justice agencies' compliance with the Code, creating the conditions to help ensure that victims receive the Code rights they are entitled to. Additionally, Ministers, having consulted with the Victims' Commissioner, may issue 'non-compliance notices' to specified criminal justice bodies if they consider their Code compliance to be unsatisfactory.
48. The policy intent at the time the VAP Act was introduced was for Police and Crime Commissioners (PCCs) to take a pivotal role in keeping under review whether and how criminal justice agencies in their police area provide services in line with the Code, and to share certain information and reports on compliance with the Ministry of Justice. Since Royal Assent in May 2024, large scale reforms to the local delivery landscape have been announced by the Home Office, most notably, the intention to abolish PCCs from May 2028. The MoJ is working closely with the Home Office to consider the impact of policing reforms on the VAP Act and on our policy intent and design of the Code compliance framework. This is essential to ensuring that the framework will work as designed, and that any necessary legislative changes to bring its statutory basis up to date are made.
49. The MoJ has been continuing to work towards implementation of the Code compliance framework. In particular, a cross-system data improvement programme has been mapping victims related data held on criminal justice systems to develop the 'metrics' that agencies will be required to collect and share under the Code compliance framework. In addition, a programme of data

improvement is underway to improve the quality of the underlying victims' data held on criminal justice data systems. This work is foundational in ensuring that once commenced, agencies are able to gather data necessary to demonstrate the extent to which they are complying with the Code.

Monitoring of the victim journey / System fragmentation and ownership

50. The MoJ recognises that victims can experience the criminal justice system as fragmented, with multiple contact points as the case moves through the system and information provided to victims in differing ways. Behind this, vast amounts of manual interventions into systems are required by staff as a case is handed off across different agencies.
51. The Government is investing in data and digital opportunities to improve how victim data is managed and used across the criminal justice system, and to improve victims' experiences of the system. Through the Connecting Criminal Justice Data Programme, the MoJ and Home Office are working to improve the quality, completeness and flow of victim data across the system. This includes improving the data needed to support victim services, Victims' Code compliance reporting and wider analysis, as well as exploring the viability of a 'Justice ID' to link offender and potentially victim information more reliably across systems so that victims, and the staff who support them, access joined up information.
52. The MoJ is also leading data-linking projects to understand 'what works' in improving victims' experiences and engagement with support services.
53. The MoJ is ensuring that any improvements to data sharing must be supported by strong effective safeguards. These are essential to ensure personal data is handled lawfully, securely and proportionately, with a strong focus on minimising unnecessary circulation of sensitive information.

Single hub / independent advocate

54. The MoJ welcomes the evidence to the inquiry provided by Claire Waxman, in her capacity as Victims' Commissioner and various reports published in her former capacity as London Victims' Commissioner, for a single 'hub' model as a central point of contact, independent of investigative agencies, to act as a "troubleshooting"

interface across police, CPS and courts, reduce withdrawal from proceedings and improve victims' experience⁵⁷.

55. There are significant issues to be explore about how a hub would interact with advocates and existing roles without creating confusion or overlap and who would hold and manage integrated victim data and whether the model requires legislation underpinning it or could be piloted administratively. Importantly, hubs should not make the information landscape more fragmented and lead to further complexity for agencies, in turn worsening the victims' experience.
56. The challenge at the heart of this issue is to consider any single point of contact (SPOC) model in the context of victims not being a party in criminal proceedings, and that judicial and prosecutorial independence limits information sharing and cross-system working in a way which can benefit the victim (over the rights of the defendant and the public interest for a fair justice system). It is within this context that any hub or SPOC model would need to be considered.
57. The MoJ submits that this issue raises a legitimate and important question for the Inquiry. The current system is not delivered through one department, and agencies operate with varying degrees of independence. Notwithstanding these complexities, it would appear that there may be merit in exploring a model which provides a consistent point of contact, improves communication and delivery of rights, and supports navigation of a fragmented system.
58. Any such model must preserve independence from operational agencies and avoid duplication of existing roles. It must also be clearly defined and practically deliverable.
59. The MoJ therefore does not resist consideration of such a model but submits that further design work would be required to ensure it is achievable.
60. Should the Chair be attracted to the provision of such a service or tool then consideration may need to be given to how realistic it is for any 'hub' to extend to health and wider services and whether the MoJ is an appropriate lead department, or whether a cross-government model is required.

⁵⁷ Evidence of Clare Waxman [INQT0000111], 5th June 2026 (AM), 35/1–36/18

Advocacy and support provisions

61. The MoJ has published guidance on Independent Domestic Violence Advisers⁵⁸, Independent Sexual Violence Advisers⁵⁹ and Independent Stalking Advocates⁶⁰ (IDVAs, ISVAs and ISAs) following evidence provided by the sector of the need for greater consistency in these roles.
62. The Government is also committed to ensuring families bereaved by homicide receive the support they need to help them build resilience to cope with the impact of these devastating crimes and this is why the MoJ commissions the National Homicide Service, delivered by Victim Support, to provide tailored, needs-led support. The service offers a consistent level of support across England and Wales and is available for as long as families require it, recognising that the impact of homicide can be long term and the needs of families can evolve over time. For 2026/27, approximately £6.7 million of funding has been provided to deliver this service.
63. The Homicide Service provides comprehensive emotional support to help stabilise families in the immediate aftermath of a homicide. Alongside this, it provides practical support to assist with immediate needs, including help to deal with agencies, manage financial and administrative tasks, and access relevant support and services including financial assistance, compensation schemes and specialist support where appropriate. The service continues to provide this comprehensive emotional and practical support through key stages such as investigations, trials and anniversaries. Support is needs-based and delivered by a dedicated caseworker; caseworkers can also arrange access to specialist support, including counselling and therapy.
64. The service includes an advocacy function, with caseworkers supporting families to understand and exercise their rights, and to navigate the criminal justice system. This includes liaison with police, the CPS and other agencies, support through legal processes such as trials, inquests and parole hearings, and assistance in accessing legal advice and statutory reviews where appropriate.

⁵⁸ Independent Domestic Violence Adviser Guidance - Statutory Guidance [RLIT0000125]

⁵⁹ Independent Sexual Violence Adviser - Statutory Guidance [RLIT0000126]

⁶⁰ Independent Stalking Advocate Guidance - Statutory Guidance [RLIT0000127]

65. Additionally, the Homicide Service also offers peer support, including one-to-one, group and online provision, enabling bereaved families to seek advice and support from others who have experienced similar circumstances. There is a specialist provision for children and young people, including a dedicated service offering age-appropriate casework support and targeted interventions to help them cope with trauma and reduce longer-term harm. Importantly, the service provides continuity of support, with families supported by the same caseworker wherever possible, for as long as needed and allowing families to rejoin the service if their needs change. All support is delivered in line with a trauma-informed approach, with staff and peer supporters receiving appropriate training and clinical supervision to ensure they can effectively support individuals experiencing trauma and complex bereavement.

The Mental Health Review Tribunal (MHRT)

66. The First-Tier Tribunal is administered by HMCTS but is itself an independent judicial body. HMCTS supports the running of the jurisdiction, but decisions made by the Tribunal are judicial decisions under the Mental Health Act and the relevant Tribunal Procedure Rules.
67. The presumption of privacy within these hearings is provided for within the Tribunal Procedure Rules as determined by the Tribunal Procedure Committee. Hearings are held in private by default because they explore matters of confidential sensitive clinical evidence, personal information, third-party information and require a balancing of the important issues of stigma and privacy. The Rules do allow for a hearing, or parts of it, to be held in public where it is in the interests of justice to do so. There also already exists provision for certain individuals to attend as 'Interested Persons' and for disclosure of documents where the requisite legal tests are met.
68. The existing framework does allow for the involvement of victims and bereaved family members, and they may make representations about a number of issues including discharge conditions. The system does allow victims in the Victim Contact Scheme, where their offender is subject to a Section 37 Hospital Order with Section 41 restrictions to provide a Victim Impact Statement. Victim Impact Statements may be considered by the Tribunal, although they do not form part of the statutory test to be applied for discharge.

69. The 2025 Practice Guidance⁶¹ incorporates a process for victims in restricted patient cases to request the Tribunal's reasons for discharge and the Tribunal will determine such a request with a view to balancing the principles of open justice with patient confidentiality.
70. The MoJ has listened intently to the evidence of Julian Hendy and his views regarding the MHRT process and these have been and will continue to be reflected upon. However, the description of the MHRT as secret courts⁶² is not accepted by the MoJ. The position can more accurately be described as one which is and needs to be private by default, but which can be more open on a case-by-case basis where the Tribunal considers it to be in the interests of justice to do so. Confidentiality is a legitimate and important principle.
71. Should the Chair be minded to make any recommendations in respect of these processes then as the body responsible for tribunal policy and administration, the MoJ accepts that it should be properly involved in any review of MHRT procedures or reform, if required, and that this will involve both justice and health considerations. The MoJ will consider and engage with any recommendation to review disclosure practices, improve communication and ensure confidence in tribunal processes.
72. Finally, on this topic, any matters of clinical care, treatment, risk assessment, medication, bed availability and length of detention are not matters that sit with the MoJ and will variably be matters for other departments including the DHSC, NHS England, various NHS providers locally and the CQC.

Concluding remarks

73. The MoJ invites the Inquiry to find that the unauthorised access was serious and has been properly scrutinised. There has been reflection on both individual misconduct and some systemic weaknesses, including access control and communication. There was a significant failure to inform the bereaved and survivors of what happened with their data.

⁶¹ Practice Guidance No. 2 of 2025 dated 27 May 2025: Practice Guidance on Procedure for Handling Representations from Victims in the Mental Health Jurisdiction of the Health, Education and Social Care Chamber [RLIT0000108].

⁶² Evidence of Julian Hendy [INQT0000100], 28th May 2026 (PM), 41/7-11; First Statement of Julian Hendy [WITN0258001] at para. 165-170.

74. Substantial reforms have been implemented so far but if it is felt that further work is required by the MoJ and its Executive Agencies then the MoJ would support recommendations that are evidence based, proportionate and capable of practical implementation.
75. The MoJ accepts that these events should not have occurred. The central issue now is not contesting what has happened, but ensuring that lessons are learned, systems undergo any feasible and practical improvement, and that public confidence is restored. The MoJ is committed to that outcome and stands ready to assist in implementing any recommendations arising from this Inquiry.

Emma Zeb KC (Gatehouse Chambers)

Tomas McGarvey (2BR Chambers)

Mark Erridge (Gatehouse Chambers)

14 August 2026