MOD data breach – Record of ICO involvement in the data breach announced by the MoD on the 15 July 2025

1. This paper sets out a record of what occurred since the MOD notified the ICO of a serious data breach on 17 August 2023, up until 10 July 2025, when the MoD confirmed to the ICO that the incident would be made public. The paper provides detail on:
    a. The handling restrictions the ICO was subject to during this period, which restricted our ability to share information more widely across the organisation.
    b. The approach adopted by the ICO to supporting and overseeing the MoD's internal investigations.
    c. Some of the key reasoning behind the decision to take no further action at that time in relation to the data breach.

Classification & Handling restrictions

2. It is important to note:
    a. Only five staff in the ICO, all of whom were approved by MoD, were formally "read on" to this matter by the MoD. Those were:
        i. Stephen Bonner (then Deputy Commissioner, Regulatory Supervision – "SB")
        ii. FOIA s.40(2) - Personal data that doesn't fall under s.40(1)
        iii. [redacted]
        iv. [redacted]
        v. [redacted]
    b. Only those staff who were formally "read on" by the MoD were able to attend in-person briefings with MoD on this issue. Furthermore, much of the information relating to the data breach was classified as Secret or Top Secret, with the MoD restricting access to this information, only showing it to ICO staff who had the necessary clearances. In practice this meant only [redacted], [redacted] and SB were able view information relating to the incident that was highly classified. [redacted] involvement focused on the comms

approach to be adopted following the lifting of the superinjunction. This high classification meant that:

i. The ICO was unable to record information regarding this data breach on ICO IT systems.

ii. All of the briefings between the MoD and ICO were face to face at MoD's offices in London. This reflected the fact that the ICO does not have the facilities to have highly classified briefings in our own offices (or attend such briefings remotely).

iii. The ICO was unable to take any written notes from the briefings with the MoD, as that would have likely necessitated the inclusion of information which was classified as Secret or Top Secret, creating additional handling difficulties.

iv. The MoD confirmed that the ICO was unable to remove evidence/copies of information from the MOD and had to review in situ.

c. In addition to the security classification of this incident, the MoD obtained a wide-ranging injunction, referred to as a "super-injunction", on 1 September 2023.

i. The MoD successfully kept the injunction in place until July 2025, with the MoD providing the ICO with updated court Orders as the matter progressed.

ii. The injunction named the ICO and made clear that it did not prevent the ICO from taking any steps in private that the ICO considers appropriate. However, the injunction explicitly prohibited (without leave of the court) the ICO publishing or making any external disclosures of information about the data breach.

iii. Given the injunction did not prevent the ICO progressing inquiries with or seeking assurances/information from the MoD, it was not necessary for the ICO to seek leave from the court to vary the terms of the injunction.

d. As a result of the superinjunction being in place and the classification of the material being discussed (detailed above), there was no internal record of the ICO's actions and decision making regarding this data breach. This record has been drafted

in July 2025, following the MoD's announcement of the lifting of the superinjunction, which has enabled us to share some information more freely with colleagues across the ICO and recorded on ICO IT systems. In absence of any contemporaneous records, the authors have used personal memory of in-person briefings with the MoD and internal ICO meetings (as well as calendar invites etc.) to draft this record.

3. Despite the lifting of the super-injunction, there continues to be information known to the authors that is unable to be included in this paper due the classification of the material. All material known to aid decision making that can be included in this record at "Official Sensitive" has been.

Summary of events and the ICO's involvement

4. For ease of reference, a brief timeline of events following the notification from the MoD about this incident is provided below at **Annex A** to this document. However, additional information regarding the ICO's involvement on this matter is detailed below.
5. FOIA s.40(2) - Personal data that doesn't fall under s.40(1) contacted FOIA s.40 by telephone on 17 August 2023, to advise of a serious data breach which required a face-to-face briefing. The ICO was notified within 72 hours of the MoD becoming aware of the breach, as required by Article 33(1) of the UKGDPR. However, given the sensitivity of the matter, it was not possible for the MoD to provide additional information at this time.
6. FOIA s.40(2) attended the MOD in London on 8 September 2023 when he was served with the superinjunction by the MoD. The injunction did not include facts/details of the matter but instead focused on information about reporting restrictions, including the restrictions on the ICO (detailed above). The rationale for the MoD obtaining the injunction was not shared at this time.
7. However, at the meeting on 8 September 2023 FOIA s.40(2) received an oral briefing of the incident, providing an overview of what was known by MoD at that time. In addition to issues which cannot be detailed in this paper due to classification, this briefing included the following information:

a. On 15 August 2023 the MoD was made aware that part of a spreadsheet had appeared online and it was understood this was an extract from an MoD dataset. It was confirmed that it was a screenshot of data from a spreadsheet (rather than an extracted file), including personal data from Afghan individuals who were part of the Afghan Relocations and Assistance Policy (ARAP).

b. The MoD's initial investigation considered whether this information had been hacked from MoD systems (Cyber related) or sent purposely with criminal intent. The MoD advised that neither occurred in this instance.

c. The MoD's investigation had confirmed that the dataset that appeared online was part of a spreadsheet which was intentionally emailed externally. The MoD explained that an email with the spreadsheet attached was sent by the MoD externally to a trusted source. The extract which appeared online, however, was part of hidden data unintentionally included within the intended dataset. In other words, the MoD intended to send the spreadsheet externally but had not intended to include the hidden data.

d. MoD wanted to understand more about the circumstances of the breach, track down the dataset after it exited MoD systems and ensure suitable safeguards could be arranged for affected data subjects.

8. Following the briefing and having been served by the MoD with the superinjunction, [redacted] understood the need for additional support within the ICO. [redacted] was aware [redacted] had a good working relationship with SB and with SB being [redacted], [redacted] requested he was read on to build resilience and provide ICO Executive Team oversight and support during this process. MoD agreed and this was arranged.

9. Following SB being formally read on to the incident by the MoD, [redacted] and SB discussed the ICO approach. SB decided that the ICO would not be in a position to independently investigate the incident at this time, which reflected the handling restrictions that the unprecedented superinjunction put in place and the fact all material was being classified at Secret or Top Secret.

10. Despite the inability of the ICO to conduct an effective independent investigation at this time, SB and [redacted] were reassured that there was a dedicated team of MOD investigators who would progress an internal

investigation. SB decided that the ICO would review, oversee and propose lines of enquiry to the MoD's internal investigation team. The MoD DPO team would be the conduit for sharing information from the MoD's internal investigation team and provide ICO lines of enquiry to be covered by the MoD.

11. On the 5 December 2023, SB and [redacted] briefed John Edwards (Information Commissioner – "JE") at a high level, explaining the ICO's approach to overseeing the MOD's investigation, but not discussing the nature of the breach itself, as the details were classified as Secret or Top Secret and only SB and [redacted] had been formally read on to this incident by MoD at this time.

12. As time went on (see timeline at Annex A), [redacted], in agreement with SB, requested additional ICO staff be read on formally by the MoD, namely [redacted] and [redacted] subsequently requested (21 August 2024) that legal resource with appropriate security clearance was formally read in on this incident by the MoD. [redacted] was identified as the appropriate person in the ICO Legal Service.

13. As a result, the MoD's internal investigation took place and additional meetings took place between the ICO and the MoD. After [redacted] initial briefing with the MoD in September 2023, SB and [redacted] attended MOD on several occasions, with [redacted] and [redacted] also joining [redacted] for in-person briefings with the MoD (see Annex A and information below).

14. These meetings were coordinated by the MoD's DPO's office, with a member of the DPO team always in attendance, either [redacted] or [redacted] [redacted] The MoD DPO's office arranged for other MoD staff to attend as necessary to provide additional confidential briefing. In these meetings, the ICO was provided with further information relating to the data breach, including:

    a. Updates on the status of the injunction, as the continued operation of the injunction was a crucial issue given the handling restrictions it imposed.

    b. Updates on the MoD's internal investigations – including the steps it was taking to mitigate the breach and safeguard individuals.

    c. Information regarding the technical and operational measures the MoD had in place already to ensure appropriate handling of sensitive information and details regarding additional measures

that were being put in place to minimise the risk of similar breaches.

15. The ICO used these meetings to critically review evidence, where necessary challenging the internal investigation team and DPO team, proposing lines of enquiry and discussing next steps.

16. Since June 2024 the ICO has had in-person briefings with MOD on the following dates:

a. <u>26 June 2024</u>

i. SB and [redacted] attended a meeting with [redacted] and [redacted] to discuss the internal investigation carried out by the MOD. [redacted] recalls recommendations to improve compliance being presented by the MoD to the ICO and SB and [redacted] agreed they were sensible. That said, SB and [redacted] felt there were still enquiries outstanding and sought confirmation in writing of the measures adopted by MoD, which [redacted] noted.

ii. [redacted] responded to these enquiries in correspondence on 8 October 2024 to [redacted] ICO email address.

b. <u>15 August 2024</u>

i. [redacted] and [redacted] read into the matter. [redacted] requested an update on enquiries from 26 June 2024 meeting. [redacted] advised [redacted] was collating responses and confirmed that the MoD will be in touch with the ICO in due course.

ii. An initial response was sent by the MoD to [redacted] and SB on 8 October 2024 (**Annex B**) – which confirmed that:

1. The MoD's DPO team had reviewed the policies and guidance in place at the time of the incident, including the Defence Instructions and Notices ("DIN"). The MoD shared extracts of the DIN which showed that MoD was aware of the risks of sharing data and explicitly referenced the need to remove hidden data from datasets.

2. There was also a separate MoD policy on removing hidden data, published in January 2017, which provided clear rules on removing hidden data. Although this policy did not explicitly reference

spreadsheets, it was guidance that was applicable to all documents shared by MoD.

3. Detail was provided on the risk registers and steps MoD has taken (after the incident) to warn users when sending data outside the MoD.

iii. Following the receipt of this information, [redacted] sent a further e-mail on the 15 October 2024 (copying in SB), asking some further questions and requesting for [redacted] to be formally read on by the MoD.

c. <u>14 November 2024</u>

i. [redacted] and [redacted] attended a meeting with [redacted] and other MoD officials. [redacted] was being formally read on to the matter and was able to ask initial questions regarding the incident. [redacted] provided updates on the MoD position and the ongoing injunction. The ICO requested a response to the outstanding issues raised in [redacted] previous e-mail of the 15 October 2025 and the MoD confirmed a response would follow.

ii. The MoD provided a further response to [redacted] and SB on 2 December 2024 (**Annex C**) – which also annexed a number of additional documents. This letter included:

1. Confirmation that Data Protection Impact Assessments (DPIAs), risk and issue registers and User Security Operating Procedures (covering Outlook and the sharing of personal data through emails) were in place at the time of the incident. Copies of these documents were annexed to the letter.

2. Extracts from a risk and issue register created for the Afghan Relocations and Assistance Policy (ARAP) units in October 2021 (prior to the incident) were shared. This showed that the MoD had documented and understood numerous risks, including the risks of personal data being compromised and the risk of data breach via e-mail.

3. Details were provided on MoD's approach to data protection awareness and training. This included

information (policies and guidance) being provided to employees at induction and annual mandatory data protection training. MoD explained that training has been updated following this incident to reflect the need to conduct risk assessments.

4. Updates were provided on changes that were implemented in 2022, after the incident occurred, but prior to the MoD becoming aware of the breach. This included:

    a. May 2022 – the introduction of a new casework management system known as the Defence Afghan Casework System (DACS), designed to move the unit away from relying on Excel spreadsheets to manage applications from individuals in Afghanistan.

    b. An Information Manager and Information Support Officer being recruited in July 2022 and January 2023.

d. <u>29 January 2025</u>

    i. [redacted] and [redacted] attended a meeting with [redacted] and other MoD officials. A general update on the status of the injunction was provided and [redacted] and [redacted] posed further questions of MoD. MoD requested some advice [redacted] confirmed he would follow up in writing, which he did on 31 January 2025.

e. <u>6 May 2025</u>

    i. [redacted], [redacted] and [redacted] attended a meeting with [redacted] and other MoD officials. At this meeting the ICO raised additional questions about the MoD's approach to sharing data externally with third parties, seeking to understand what mitigations the MoD had put in place (given this type of data sharing would continue to be necessary in some circumstances). We also discussed the ongoing question of

the injunction and had the opportunity to briefly review some of the MoD's proposed comms lines.

ii. After not receiving a response to the latest enquiries, [redacted] followed up with [redacted] on 3 June 2025. On 4 June 2025, [redacted] emailed a list of outstanding actions, which sat with MoD.

iii. Ultimately the MoD responses to some of the queries raised at this meeting were not provided to the ICO until its letter of 10 July 2025 (**Annex D**). This letter included:

1. Information about changes implemented by the team in MoD responsible for the breach since the MoD became aware of the incident.
2. This has included system changes, additional training (including workshops), updated data handling policies and establishing a dedicated "Data Team" (responsible for governance and risk management).
3. This letter also pointed to an external data protection review (the "McIvor Review"), which was conducted by a member of the Senior Civil Service from the Department for Education in January 2024. The MoD maintained that these findings demonstrated its progress in addressing the ICO concerns.

Communications strategy regarding the data breach

17. In addition to discussing the substance of the data breach and the MoD's investigation, the ICO also had discussions with the MoD regarding the proposed communications and engagement strategy, in the event that the injunction was removed and information relating to the breach was made public.

18. On 3 July 2024, [redacted] sent an initial comms and engagement pack to the ICO via e-mail on a cross-government technology platform to [redacted] In the ICO only specified individuals have e-mail accounts on this platform. On multiple occasions [redacted], [redacted] and [redacted] viewed the information shared by the MoD on this platform.

19. On 30 August 2024, [redacted] and [redacted] met in the ICO office in Wilmslow to draft comms lines.

Security classification: OFFICIAL SENSITIVE

20. On 19 September 2024 [redacted] and SB met internally to discuss the approach the ICO should take to communications regarding this incident and to review the drafts [redacted] and [redacted] created on 30 August 2024. SB decided that the ICO was unable to take regulatory action at this time, but that the ICO were also not in a position to finalise press lines as we were still waiting for additional information from MoD. This position was communicated to JE later that day (see below for more details).

21. As a result of the above, the ICO's holding lines created made clear that while the ICO had supported the MoD's internal investigation, the ICO could not provide full assurance of an outcome. Due to the injunction and handling restrictions, this draft remained on the cross-government technology platform.

22. The media lines continued to be reviewed by [redacted], [redacted] and [redacted] following the subsequent meetings between the ICO and MOD (as detailed above and in the timeline at Annex A).

23. On 19 May 2025, the ICO received a media enquiry that appeared to relate to this matter. A holding line was issued to the journalist in question. [redacted] spoke to [redacted] by telephone on 19 May 2025. On that call, the MoD informed the ICO that 'break glass' could happen in approximately six weeks.

24. The ICO sent a number of e-mails to the MoD over the following five weeks, requesting updates on the outstanding enquires and the lifting of the superinjunction. This included an e-mail from [redacted] to the MoD on the 8 July 2025 to confirm that the ICO may not be able to provide clarity on the ICO's position in comms lines while we are still waiting for additional information from the MoD.

Decision – June 2024

25. Prior to the MoD confirming to the ICO on the 10 July 2025 of the "break glass" event on the 15 July 2025, SB was the only member of the ICO's Executive Team who had been formally "read on" by MoD into the incident. SB's role as Deputy Commissioner included responsibility for leading supervisions and enforcement matters across the ICO. Due to handling restrictions, no other members of the ICO's Investigations leadership team were made aware of the incident. As a

result, for this matter, SB was the primary decision maker regarding the ICO's approach to regulatory supervision.

26. SB was content that while the super-injunction was in place and much of the material remained at Secret or Top Secret, it was not possible to formally and independently investigate the matter. This was necessary due to the extremely limited number of [redacted] staff and practical challenges of investigating highly classified matters.

27. Following briefings and reviews of documentation from MoD in situ, SB's view, communicated orally to [redacted] on the 26 June 2024, was that based on the information available to the ICO, no further action ("NFA") was required at that time. This was initially discussed after the in-person meeting at MoD on 26 June 2024, with the caveat being that what we were advised in this meeting was subsequently confirmed by the MoD.

28. SB's decision to take NFA at that time was later communicated at a high level to JE in person on 19 September 2024. This was communicated to JE who had no objection with the approach.

29. There were a number of factors that were relevant when SB took the decision for NFA at that time. These factors are summarised below based on the recollection of [redacted], sharing relevant information which can be shared at Official Sensitive classification. When [redacted] was read on formally by MoD in November 2024, these issues were also discussed with him as reasons for the ICO's decision of NFA at that time.

Injunction and ongoing handling restrictions

30. As detailed above at paragraph 2, the fact of the super-injunction being in place and the classification of material (most of which was at Secret or Top Secret) meant that it was not feasible for the ICO to stand up an independent investigation at that time. While the injunction did not prevent the ICO taking appropriate steps internally to consider the breach, the classification of the material placed real limits on the ICO's ability to consider and assess information.

31. Ultimately the MoD was continuing to conduct an internal investigation into the incident. That investigation had the benefit of unrestricted access to classified information and benefitted from significant resource. As a result, at that time, it made sense for the ICO to focus its efforts on supporting the internal

investigations/reviews, proposing lines of enquiries and raising concerns/issues as they emerged.

Pro-active approach MoD took to engagement

32. The MoD notified the ICO within 72 hours of becoming aware of the data breach in August 2023, complying with the requirement in Article 33(1) of the UKGDPR. Following the initial notification, MoD sought to provide detailed briefing to the ICO. This approach reflected the fact that, despite the sensitivity of this matter and the MoD's decision to get a super injunction, it was not seeking to avoid scrutiny or oversight from the ICO.

Date of incident and other investigation into MoD

33. Another key factor in the decision for no further action at this time is when the incident took place. It is noted that the disclosure of information, including hidden data, took place during February 2022. While it is acknowledged that hidden data isn't a new or novel concept, the ICO was informed in August 2023, at which point we were already investigating and taking regulatory action against the MoD for a separate data breach. The other breach, reported by the MoD to the ICO in September 2021, involved the email addresses of individuals being inadvertently placed in the "To" field of an email instead of the "blind carbon copy" ("BCC incident"). The ICO imposed the fine for the "BCC incident" in December 2023.

34. As part of the investigation into the BCC incident, the ICO was updated on the changes adopted by the MoD since the incident in 2021. This investigation showed that the incident was not reflective of systemic failings at the MoD. Furthermore, the MoD had already undertaken an independent review of data protection governance, so it was concluded that there was limited value in the ICO seeking to conduct a further review. This was a key part of the decision to take no further action at that time in relation to the spreadsheet breach.

Risk of harm and the impact on individuals

35. Throughout discussions with the MoD, the risk of harm to the thousands of Afghans whose information was wrongly shared and the

potential impact on their lives has been a key priority for the ICO and the risk of harm was extremely serious.

36. However, we received briefing from the MoD on its attempts to assess risk to individuals and the measures the MoD had taken to mitigate the risk. It was clear the MoD was taking seriously its responsibility to mitigate the risks to individuals and minimise the impact of the breach on those affected.

Nature of the breach

37. The ICO understood this matter to involve one email which contained a spreadsheet, which itself contained hidden data. Information provided to the ICO suggested that the matter was a one-off occurrence following a failure to following usual checks, rather than reflecting a wider culture of non-compliance.

Urgency

38. A key consideration was the urgency in which the MoD were operating at the time the breach occurred. We understand that the MoD took the view that some data sharing was necessary in order to validate the identity of those applying to come to the UK, so there was inherently some risk that the MoD were having to take by taking the intentional decision to share some data externally in these circumstances. At the time the MoD systems were not set up for this and the MoD team was working at pace in order to identify which individuals should be supported for evacuation from Afghanistan, with the MoD assessing that there was a clear threat to life.

39. The urgent nature of the data sharing contrasts with other cases where public authorities have accidently disclosed spreadsheets containing "hidden data". For example, in the PSNI case, the police were responding to a routine FOIA request and there was no intention to share any names/personal data as part of that response (we are also aware of similar breaches by other police forces in similar circumstances when responding to FOIA requests). In the context of FOIA requests, the ICO rightly expects organisations to ensure that processes are in place to avoid inadvertent disclosure.

40. Similarly, the spreadsheet data breach is distinct from the data breach arising from the BCC incident reported by the MoD to the ICO

in 2021. The BCC incident was the result of a more "business as usual" process, sending e-mails externally. By contrast, this data breach appeared to be the result of the way in which this specific team in the MoD operated and their requirements to engage with resources and capabilities outside of the normal MoD process and practices.

Measures taken by MoD to assess and mitigate the risk

41. The MoD's DPO team provided regular updates on the steps the MoD were taking to review the teams existing training, policies and processes to ensure they were fit for purpose. The MoD explained some of the measures being adopted to minimise the risk of an incident like this occurring again. This was discussed at the in-person briefings the ICO attended with MoD, including the meeting of the 24 June 2024.

42. Ultimately the briefings confirmed that the MoD did have processes and policies in place which are designed to address the risks. The MoD also demonstrated that since the incident took place, the MoD had taken steps to implement improved systems and processes, which reflected a recognition of the need to manage the risks which had been identified.

43. The MoD subsequently provided confirmation in writing of some of the steps they have taken (letters at Annex B, C & D). The letters at Annex B and C supported the information provided to the ICO at the in-person briefings. The letter at Annex D was received on the evening of the 10 July 2025 and as a result of other demands on the ICO around the time of "break glass", we have not had the opportunity to consider this additional information in detail. However, from our initial review it appears consistent with the information provided by the MoD previously.

Steps taken by the MoD took to track the lost data

44. We received briefing (classified at SECRET or above) from the MoD on the measures the MoD had taken to try and limit loss of control of the data once the breach was identified. This included taking intensive measures to recover and delete data from all identified sources. Once the breach occurred the MoD was never going to be able to entirely

mitigate the risk of further dissemination of the dataset, but the ICO recognise the serious and resource intensive steps the MoD took in order to contain the information.

Cost of responding to the incident

45. During a face-to-face briefing, the MoD advised the ICO that this was likely 'the most expensive email ever sent'. Whilst we were not provided with specific numbers regarding the cost of their response to the breach, it was clear that it had already cost MoD hundreds of millions of pounds. While no formal investigation had been commenced, it was considered that, in line with the ICO public sector approach, further engagement with the MoD would be more effective than seeking to impose additional cost to the tax payer at this time.

Author: FOIA s.40(2) - Personal data that doesn't fall under s.40(1) **– 6 August 2025**

Security classification: OFFICIAL SENSITIVE

Annex A – ICO timeline of MoD data breach

Please note - all briefings took place at MoD, Main Building, London unless stated otherwise.

For context, reference is also made to another MoD data breach which the ICO were investigating during this period.

- September 2021 – the MoD incident involving the email addresses of individuals being inadvertently placed in the "To" field of an email instead of the "blind carbon copy" ("BCC incident").
- 21 September 2021 – the MoD reported the BCC incident to the ICO.
- February 2022 – the MoD share a spreadsheet externally.
- 15 August 2023 – the MoD become aware of the spreadsheet data breach.
- 17 August 2023 – the MoD report the data breach to the ICO. [redacted] contacted over the phone by [redacted] to advise of a serious data breach which required a face to face briefing.
- 8 September 2023 - [redacted] attended the MOD in London on 8 September 2023 when he was served with the superinjunction by the MoD.
- 5 December 2023– SB read into the matter and given overview by MoD. High level overview provided to JE later that day at ICO London Office.
- 13 December 2023 – the ICO announced their findings into the MoD's BCC incident, imposing a fine of £350,000.
- 26 June 2024 - SB and [redacted] attended a meeting with [redacted] and [redacted] to discuss the internal investigation carried out by the MOD. Enquiries made by [redacted] and SB.
- 26 June 2024 - SB's view (communicated orally to [redacted] was that based on the information available to the ICO, NFA was required at that time, with the caveat being that what we were advised in this meeting was subsequently confirmed by MoD in writing.
- 15 August 2024 – [redacted] and [redacted] read into the matter. [redacted] chased enquiries from 26 June 2024.
- 3 July 2024 - [redacted] sent initial comms and engagement pack to [redacted] on the cross-government technology platform.
- 30 August 2024 – [redacted] and [redacted] drafted ICO comms lines in ICO Office in Wilmslow on the cross-government technology platform.
- 19 September 2024 – [redacted] and SB met to discuss ICO approach to comms. SB agreed that the ICO was unable to take regulatory

action at this time, but that the ICO were also not in a position to finalise press lines as we were still waiting for additional information from MoD. This position was communicated to JE later that day in ICO Wilmslow Office.

- 8 October 2024 – response to enquiries from 26 June 2024 received from MoD.
- 14 November 2024 – [redacted] read into the matter. Update provided by MoD to [redacted] and [redacted]
- 29 January 2025 – [redacted] and [redacted] attended update meeting with MoD. [redacted] and [redacted] made further enquiries and MoD requested advice [redacted]
- 6 May 2025 – [redacted] and [redacted] attended update meeting with MOD. Comms lines on break glass discussed and further enquiries posed by ICO.
- 19 May 2025 – ICO received a media enquiry potentially relating to this matter. [redacted] spoke to [redacted] over the phone, who advised break glass was expected to happen in 'about 6 weeks'.
- 3 June 2025 – 5 June 2025 – Emails between ICO and MoD re comms meeting and outstanding enquires
- 5 June 2025 – SB 'read off' at MoD Main Building, London.
- 16 June 2025 – MoD emailed ICO to advise of a potential claim from Baring Solicitors. [redacted] acknowledged and requested an update on comms meeting and outstanding enquiries.
- 8 July 2025 – ICO sent chaser to MoD re comms meeting and outstanding enquires. MoD respond advising break glass expected to be on/around 14 July 2025.
- 10 July 2025 – MoD confirm break glass for 15 July 2025. Comms and Engagement pack provided as attachment.