



Neutral Citation Number: [2026] EWHC 1986 (Admin)

Case No: AC-2025-LON-001063

IN THE HIGH COURT OF JUSTICE
KING'S BENCH DIVISION
ADMINISTRATIVE COURT

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 31 July 2026

Before :

THE HONOURABLE MR JUSTICE MCKENDRICK

Between :

THE KING

Claimant

On the Application of

BB

- and -

**THE COMMISSIONER OF POLICE OF THE
METROPOLIS**

Defendant

Fiona Murphy KC and Alex Benn (instructed by **Irwin Mitchell**) for the **Claimant**
Saara Idelbi and Ellie Mullett (instructed by **Metropolitan Police Service Directorate of
Legal Services**) for the **Defendant**

Hearing dates: 6 and 7 May 2026
Further evidence and submissions received by 14 May 2026

Approved Judgment

This judgment was handed down remotely at 10.30am on 31 July 2026 by circulation to the parties or their representatives by e-mail and by release to the National Archives.

.....

McKendrick J :

Introduction

1. By way of a claim form dated 7 April 2025 the Claimant seeks to judicially review the Defendant’s policy entitled “*Guidance: Instant Messaging Apps (including WhatsApp) on MPS Issued Devices*” (hereafter “**the Guidance**”). The focus of the challenge is the part of the Guidance which instructs Metropolitan Police Service (hereafter “**MPS**”) employees who are using the messaging application WhatsApp, to switch on and use the disappearing chat function at ninety days after receipt of the message, without a reliable mechanism for storage. The disappearing chat function automatically deletes the conversation and any images or other data within the WhatsApp conversation ninety days after the conversation began. The Claimant submits this is unlawful and seeks relief by way of declaratory orders in respect of the Guidance, taken as a whole. The Defendant submits the Guidance is lawful and resists the relief sought.
2. There are four grounds of challenge. These are:
 - a. The issuance of the Guidance by the Defendant is unlawful because it authorises and approves unlawful conduct by those to whom it is directed contrary to *Gillick v West Norfolk and Wisbech Area Health Authority* [1986] AC 112 (hereafter “*Gillick*”); and *R (A) Secretary of State for the Home Department* [2021] UKSC 37; [2021] 1 WLR 3931 (**Ground One**);
 - b. The Guidance is unlawful as it frustrates the purposes of the Police Reform and Social Responsibility Act 2011 (hereafter “**the PRSRA**”) contrary to the principles set out in *Padfield v Minister of Agriculture, Fisheries and Food* [1968] AC 997; (hereafter “*Padfield*”) (**Ground Two**);
 - c. By issuing the Guidance the Defendant has acted unreasonably as understood by *Associated Provincial Picture Houses Ltd v Wednesbury Corporation* [1948] 1 KB 223 (hereafter “*Wednesbury*”) (**Ground Three**);
 - d. The Guidance represents an “unjustifiable interference with the Claimant’s right to a fair trial protected by Article 6 ECHR” and at common law (**Ground Four**).
3. Permission was granted in respect of all four grounds by order of Ms Sarah Clarke KC, DH CJ, dated 4 November 2025. I heard legal argument on 6 and 7 May 2026. Further

evidence was filed by the officer in the case and I directed that the parties file further written submissions on the relevance of this further evidence to the claim. The Claimant filed written submissions on 12 May 2026 and the Defendant on 14 May 2026.

4. Both parties invited me to make an anonymity order to ensure information discussed in these proceedings does not cause an unfairness to the Claimant's forthcoming criminal trial. I acceded to that application.
5. I agree with the Defendant's complaint that the Claimant's case has evolved from the pleading in its Statement of Facts and Grounds to the skeleton argument. He has not applied to amend his grounds. Against this background it is not always clear what is being argued under each ground. This was made more difficult by the direction that post-hearing evidence was necessary.
6. I have concluded the correct outcome is to dismiss all four grounds of challenge. I endeavour to set out my reasons below.

Background

7. The Claimant was arrested on 3 May 2024 on suspicion of coercive and controlling behaviour. The allegation had been made by his ex-partner, Z. Z had also made an allegation of sexual assault by WhatsApp in early May 2024. Z sought a non-molestation order ("NMO") against the Claimant, which was made on 16 May 2024. The Defendant understands the NMO was formally served on 22 May 2024.
8. The Claimant was arrested on 6 July 2024 for alleged breaches of the NMO, in that it was alleged the Claimant had contacted the complainant through Telegram and Instagram, and called her. He was charged for the same, but not charged in respect of the sexual assault allegation.
9. Detective Constable Archer is the officer in the case. DC Archer communicated with Z by WhatsApp on a number of occasions. DC Archer exported WhatsApp conversations with screenshots and a video also sent. She was required to file a further witness

statement after the hearing in this matter, to clarify her WhatsApp communication with Z.

The Guidance

10. The Guidance says it is dated August 2023. I have set out the entirety of the Guidance except for the ‘Annex I’ advice on how to export chats from WhatsApp to the repository for evidential or investigatory material, called Connect. I have added my emphasis in underline:

Guidance: Instant Messaging Apps (including WhatsApp) on MPS Issued Devices

Introduction

Instant messaging apps have been introduced to provide our workforce with the tools they need to succeed. This document is designed to outline how instant messaging apps, including WhatsApp, should be used on MPS issued devices.

Personal responsibility, common sense and high standards are essential. This document cannot legislate for every scenario but is intended to provide useful guidance to all officers and staff. The guidance will at times specifically focus on WhatsApp but all users should follow the equivalent steps on other instant messaging apps and where unsure consult the DDaT Digital Delivery Team for advice.

When using instant messaging for a policing purpose an MPS issued device must be used. Users must comply with the policies relating to the use of MPS systems at all times.

Set Up and Configuration

To maintain a consistent and professional standard all users should complete the following actions before using instant messaging on an MPS device:

1. **Image and name** – Users must set the MPS crest as their image and name as the user's full name and rank or band/role (see below image).



2. **Group chat access** – All users must change the privacy settings so that only contacts are permitted to add the user to a group chat. Users must not join any group chats that they do not recognise. Those with 'admin' rights, or similar, should not add any unknown contacts to group chats. Users are advised to periodically review and validate contacts to ensure they are known.
3. **Consent** - When joining or setting up a group chat users you must obtain consent from all members to share contact details and information with each other and record said consent on an MPS central system be that outlook or other relevant MPS IT system.
4. **Disappearing Messages (or similar function)** – When using WhatsApp users must ensure disappearing messages are selected for all chats (groups and individuals), with the message timer set to 90 days.
5. **Turn off auto-save** – Within settings, users must de-select 'Save to Camera Roll'.
6. **Privacy Settings** – Privacy settings should be considered, including whether the account is visible in respect of 'last seen' or 'online' status, and whether 'read receipts' are turned off.
7. **Out of office** – If on leave, users should change the settings so that 'away' replies are sent. In the case of WhatsApp, these can be added through Settings > Business Tools > Away Message. They should include details of when the user is due to return and be used in the same way as an email out of office message.

General Principles of Use

- **Professional Communication Standards** - tone and content of instant messaging should be considered in exactly the same way as if communicating on any workplace forum. If a user would not consider a message suitable for a work email or conversation then it is not acceptable to send on instant messaging. Communication must be professional and the Standards of Professional Behaviour applies to all messages whether sent on or off duty. If an inappropriate message is received, there is an expectation this would be reported as soon as practicable.

- **Lawful Business Monitoring** - LBM will apply to messages sent through instant messaging apps on MPS devices.
- **Personal Devices** - all MPS business must be conducted exclusively on MPS issued devices. Personal devices must not be used for work purposes.
- **Communication Tool** – WhatsApp is an option for officers and staff to use to communicate, but they are not required to use it. Careful consideration should be made as to whether it is the most appropriate tool to use, there will be instances where the use of the radio or email, for example, will be more suitable.

Instant messaging: with colleagues

Instant messaging between colleagues or groups of colleagues is permitted, provided the messaging is professional. Acceptable communication will often be logistical, regarding resource allocation, messages of support or encouragement, or non-sensitive advice and guidance. Instant messaging may also be used to arrange and coordinate work-related events. It is not possible to list every form of acceptable use and common sense and good judgment is required.

The content of instant messaging must **not** include:

- Information that would attract a protective marking of OFFICIAL-SENSITIVE or above (e.g. photos of offenders, PNC records, biometric information, intelligence etc.).
- Evidential material, or material generated in the course of an investigation which would engage CPIA retention and disclosure obligations – this would include significant updates on an investigation to victims of crime.
- Operational decision making, or a record of such decision making rationale.
- Central AID warnings or changes to duty times.

Colleagues are encouraged to think of instant messaging as a forum for short term disposable communications - similar to Microsoft Teams chat - to support the effective day to day functioning of the workplace and work relationships. Instant messaging is not a forum to create, share, record or store operational information.

Instant messaging: with the public (including stakeholders and partners)

Instant messaging can be used to contact members of the public, including stakeholders and partners. It may be a useful forum to engage with community groups or partners through individual chats, group chats, or broadcast lists. Instant messaging with victims, witnesses and suspects, for a policing purpose, is permitted and that availability of WhatsApp in particular is a positive step in making the MPS more accessible and responsive. But these communications do require particular care and attention.

Instant messaging should only be used if the member of the public indicates that it is a preferred or acceptable method of communication, and the limitations of its use (e.g. not available 24/7, not to be used in an emergency) should be discussed and understood. Consideration when sending an update should be made, being cognisant of your shift patterns. Any communication should be properly recorded on Connect, where appropriate.

Confidential or evidential material must not be shared through instant messaging. There may be times where members of the public unexpectedly send evidential material through instant messaging, or the message is believed to be of evidential value. If this occurs then the chat can be exported (see guidance in annex 1) and uploaded to Axon Capture, by the user, as soon as possible and all actions properly recorded on Connect.

A summary table for the use of instant messaging is provided below:

Contacts for instant messaging

- ✓ Colleagues
- ✓ Partners, stakeholders, community groups
- ✓ Victims, witnesses and suspects (with agreement, and care)
- ✗ Routine personal contacts – family, friends*

**it is acknowledged that on occasions there may be no other way for an individual to be contacted/or contact their family in an emergency other than their MPS issued device.*

Summary

Use of instant messaging

- ✓ Work purpose
 - ✓ Logistics and resources
 - ✓ Arranging calls, meetings and work-related events
 - ✓ Community, partner and stakeholder engagement
 - ✓ Support and welfare
 - ✓ Non-sensitive updates and advice

 - ✗ Routine personal use
 - ✗ Exchanging information or material at OFFICIAL-SENSITIVE and above
 - ✗ Generating material in the course of an investigation, or sharing such material
 - ✗ Generating or sharing evidence and intelligence
 - ✗ Operational decision making (i.e. using WhatsApp inform and record a decision or detail the rational for making one)
 - ✗ Sensitive, personal information Where a record of the contact is required, record on CONNECT (for example, arranging a time to meet a witness to take a statement).
- Where any of the prohibited uses occur, use 'export chats' function to avoid loss and save the record accordingly (see below). Seek advice or inform a supervisor where necessary.*

Defendant's Evidence

11. The Defendant has filed a number of witness statements in his defence of the claim.

Darren Scates

12. His witness statement explains that between 2023 and January 2026 he was the senior technical and data adviser to the MPS management board on matters related to digital data and technology. He sets out that the decision to roll out WhatsApp on MPS issued devices was made by the MPS executive team. He says that the decision was made by the Commissioner to provide all MPS staff and officers with smart phones. The purpose of MPS issued smartphones was to enable better internal and external communications.

The use of WhatsApp on MPS devices was reviewed in October 2022. He says the decision to implement WhatsApp on MPS issued devices was driven by the shift in public communication behaviours and the need to maximise effective engagement with communities, partners and stakeholders. He points out the decline of traditional SMS messaging and the increase in WhatsApp. He produced a paper in November 2022 in which he set out that the dual use of MPS phones for personal and professional purposes should cease save for emergency use and that the use of personal phones for policing purposes should be prohibited again except for emergencies. He said that in relation to the use of WhatsApp as a stand-alone system this would not be compliant with Management of Police Information or the Data Protection Act. But he went on to explain that the risk could be mitigated by Lawful Business Monitoring (hereafter “LBM”). He set out three policy options for the MPS: (i) stopping using all MPS staff from using WhatsApp; (ii) allowing all officers and staff access to WhatsApp; and (iii) to continue with superintendent level authorisation of WhatsApp for officers and staff who demonstrated the business need for the same. He sets out in his evidence that the first and second options were not recommended by him. He did not recommend the second option because LBM was not live across the organisation as yet. He considered the risks attached to the third option were acceptable. His paper highlighted the guidance on the use of WhatsApp as issued by the Independent Office for Police Conduct (“IOPC”). He then explains that in November 2022 there was a management board ‘Away Day’ where recommendations for WhatsApp use amongst the MPS were discussed. He sets out in his evidence that the Board noted that WhatsApp assisted frontline officers in communicating with individuals and community groups who prefer to use instant messaging as their primary means of communication. He said in his evidence that this improved the speed and accessibility of police communication and help to build trust and rapport with individuals. The Board however noted the risks associated with WhatsApp. He was therefore tasked to identify options to manage the risks of the use of WhatsApp on MPS phones.

13. In January 2023 he circulated a further policy in respect of WhatsApp use and MPS devices. Once again he recommended WhatsApp use be subject to sanction by a police superintendent. He goes on to explain that in January 2023 the Commissioner’s senior leadership team noted that it was no longer tenable to have ad hoc use of WhatsApp. It was also noted that there was a risk in not authorising WhatsApp on MPS issued

devices, because that incurred the risk of officers using WhatsApp on their personal devices which was not the subject of LBM oversight. It was agreed by the Senior Leadership Team (“SLT”) for there to be access to social media, including WhatsApp, on MPS work devices. That policy was explicit in being consistent with the terms of the Criminal Procedure and Investigations Act 1996 and the Freedom of Information Act 2000.

14. In August 2023 he sent a letter to the information Commissioner’s office setting out how the MPS was addressing the points raised by the Information Commissioner in a Data Protection Impact Assessment (“DPIA”).

James Harman

15. James Harman is a deputy assistant commissioner for police operations and has had that role since September 2025. At the time that WhatsApp was made available on MPS devices in 2023, he was the Commander for the Directorate of Professional Standards. He was responsible for the implementation of the WhatsApp user guidance. He recounts in his evidence that whilst he was not involved in the rollout of WhatsApp on MPS devices his understanding was that there was evidence that there would be greater engagement with the public, partner organisations and stakeholders if WhatsApp were used. It was also noted that superintendents within the MPS had already authorised multiple requests by officers to use WhatsApp on their MPS devices. Overall it was felt WhatsApp would improve communication with stakeholders. His evidence is that he believes in March 2023 there was a meeting to consider the implementation of WhatsApp and the need to develop in draft a user guide for MPS officers in respect of the use of WhatsApp on their MPS devices. He says that the user guide was drafted by colleagues in Strategy and Governance and that his colleague Peter Shaw explains the drafting process.

16. He explains in his witness statement that given the use of WhatsApp on MPS devices, there had to be consideration given to the length of time that data would be retained by the MPS. He was responsible for making these decisions. He was also the senior decision maker in respect of aspects of the DPIA. He says that he wanted to avoid indefinite retention of WhatsApp messages because he considered that the aggregate

amount of data of tens of thousands of officers would accumulate each year and would pose an unacceptable risk of personal data being held by the organisation in a decentralised way. He points out that the SLT intended that WhatsApp be used for logistical and practical messaging. In that context he took the view that the disappearing message function was an important safeguard to have as a default for the MPS use of WhatsApp. He then sets out that a discussion took place as to whether it should be twenty four hours or seven days or 90 days. He considered seven days was too short. He noted that officers may receive evidential material which would be material relevant to a criminal investigation and therefore would be subject to CPIA obligations. He took the view that sufficient time would be required to upload any material of that nature and he recognised officers have busy schedules and many commitments. He took the view that 90 days would provide for sufficient time for uploads taking into account rest days, annual leave or sickness and that 90 days was a reasonable balance between retaining what was needed and avoiding the retention of excessive amounts of data indefinitely. He also took the view that imposing the 90 day disappearing chat function would prompt officers to assess the data on their devices and determine at regular intervals how to process information and data on their WhatsApp, in their MPS devices. He took into account the risk that officers may forget to upload relevant material. But he took the view that that was the same for digital and physical evidence. He took the view that the fact that some officers may forget to upload relevant material was ultimately thought to be outweighed by the benefits of using WhatsApp by the MPS. He considered a variety of different options. Therefore on 19 April 2023 he amended the user guide to reflect that a 90 day WhatsApp disappearing chat function is recommended for MPS officers.

17. He then explains his involvement in the DPIA. He explains the Information Commissioner was informed in June 2023 that WhatsApp would be made available to MPS officers. The Information Commissioner responded by saying that there was no objection to the use of private messaging services like WhatsApp provided there is sufficient governance and oversight. On 19 June 2023 he sent the DPIA and the working draft of the user guide to the Information Commissioner. He points out that it was not the role of the Information Commissioner to agree with the decision-making process, or with the DPIA. He points out that when the Information Commissioner responded on 18 July 2023 they raised several questions about the use of WhatsApp within the

MPS. He notes the Information Commissioner raised questions about the 90 day deletion. He also notes the Information Commissioner raised further concerns about compliance with data access subject rights and the high risks to the rights and freedoms of individuals. The MPS made clear that central searching of WhatsApp messages by officers would not be possible at the date at which WhatsApp would be deployed to the MPS officers. The DPIA was sought to be finalised in August 2023 because it required sign off by senior management. It was noted that not all of the Information Commissioner's concerns could be met. He prepared a paper for the management board in August 2023. He noted one of the risks identified was that WhatsApp does not have a central repository, with the result that searches within the 90 day window would not be possible. On 4 August 2023 the MPS management board approved the rollout of WhatsApp to all MPS devices with a start date of 1 September 2023. He says that on 24 August 2023 he wrote noticing that the National Police Chiefs' Council ("NPCC") had provided advice to chief constables in January 2023 cautioning against the risks inherent in the use of WhatsApp. However he noted that the MPS considered the benefits of WhatsApp outweighed the risks. He repeated the rationale for the 90 day retention window prior to automatic deletion.

Pete Shaw

18. He explained he is a chief inspector in the MPS. He explains that in February 2023 he was asked to develop a user guide to accompany the rollout of WhatsApp on MPS devices. He said that as this was developed it was noted that WhatsApp would not be used as an investigative tool. He explains that from April 2023 he began engaging with external stakeholders such as the Information Commissioner, the Mayor's Office for Policing and Crime; the National Police Chiefs' Council; and also the Independent Office for Police Conduct. He says as he drafted the user guide, his team considered various policies produced by these various organisations including also Baroness Casey's review into the standards of behaviour and internal culture of the Metropolitan Police Service.
19. He explains that he was the tactical lead for the drafting of the DPIA. The DPIA was produced as an iterative process of updating and refining. He said the DPIA was formally completed and signed off by Commander James Harman on 9 October 2023.

After the issue of WhatsApp he conducted a post-rollout survey about officers' experience of WhatsApp on MPS devices. Over 750 responses were received. It appears the case that the user guide was clear and helpful.

David Millyard

20. He explains that he is a detective sergeant with the MPS. He explains what an LBM is. He explains that an LBM refers to authorised monitoring of an organisation's IT system and communication for legitimate business purposes to prevent and detect crime or misconduct and to ensure compliance with policies and standards to maintain public trust and accountability. He explains that data collected by the LBM is currently retained for two years before it is automatically deleted. He says that the current DPIA will seek to increase the retention of all LBM data including WhatsApp data to 6 years and that this awaits legal sign off. For the MPS, LBM involves the use of software called App X. He explains a significant amount of detail about the proof of concept to test the capability of App X. He explains that he tested App X from January 2023 and notes that App X appear to capture the functions of WhatsApp that he expected MPS officers might use or misuse. He explains that App X was rolled out across MPS' devices in September 2023 but notes that as of December 2023 there was a low take-up of around only 14%. He sets out that this was probably because of a lack of knowledge about App X and a lack of technical expertise. He explains the MPS have taken steps to improve compliance with App X activation. He explains as a result of this, by January 2026, 94% of MPS devices had App X activated. He goes on to explain that he tested the disappearing chat function on WhatsApp in the context of App X from September 2025. He notes that disappearing WhatsApp messages would not be captured by App X until those messages had been viewed on the smartphone in question. He points out that he was not concerned that messages sent but not viewed which then disappeared were not an issue from his perspective.

Maria Archer

21. She explains that she is a detective constable with the MPS. She sets out her background training and understanding of the CPIA and of the suite of MPS' policies on information technology and data retention. She goes on to explain that she is the officer in charge

in the case of BB. She explains that the Claimant faces a trial on indictment for one count of engaging in controlling and coercive behaviour in 2024 and three counts of breaching a non-molestation order. She explains that the trial is due to start in November 2026.

22. She explains that in May 2024 the complainant, Z, attended Charing Cross police station to report BB for harassment and stalking. A variety of background details and information regarding the allegations made were recorded. She explains officers met with Z and took a statement from Z and created a crime reference number. She was then appointed the officer in the case. She explains from notes that her first contact with Z was on a telephone call on 2 May 2024. Z alleged that BB was attempting to make contact via an app called Revolut. DC Archer asked Z to take screenshots so this could be evidenced. She cannot recall if she explained to Z how to share the screenshots or whether she said that WhatsApp should or should not be used for sharing this information. She explains that around an hour after the telephone call Z sent the evidential screenshots to her using WhatsApp. She explains that she exported this chat on 20 May 2024. She explains that she would have taken clear steps to discourage Z from sending evidential material via WhatsApp. After the screenshots were received, she explains she would have told her to send evidence via evidence.com rather than via WhatsApp. She goes on to explain that evidence.com ensures retention of relevant material. She explains she did not turn off the disappearing message feature but she was alert to the need to export any evidential material received from WhatsApp. She went on to explain BB was arrested and interviewed on 3 May 2024. He was released on bail on 4 May 2024. She then used WhatsApp to update Z on the case. She continues explaining a number of examples of communication she had via WhatsApp with Z in May. She goes on to explain she did not export any of these messages at the time because she did not deem them to be relevant material but she did add the particulars to the case file.

23. On 20 May 2024 she had a telephone call with Z in which she asked whether any sexual activity had taken place between BB and Z. After the call she received WhatsApp messages from Z stating that she believes she may have been raped. She goes on to explain that she immediately used the export chat function on WhatsApp to export the chat with Z. She exported the full chat including the disclosure of rape. She goes on to

explain she is not able to identify messages sent before 20 May which she did not consider to be relevant because she exported the full chat. She created a separate crime report for the rape allegation. She explains in her witness statement she cannot recall if the user guide was a relevant factor in her decision to export the WhatsApp chat but the purpose of exporting the chat was to create a permanent record of relevant material. She goes on to say that she considered the contents of the WhatsApp conversation with Z to meet the definition of relevant material for the purposes of the CPIA. She said it was relevant to the investigation because the disclosure was linked to the surrounding circumstances of the case that is to say coercive and controlling behaviour including sexual abuse. She also says it was relevant to the rape allegation. She explains that after 20 May 2024 Z sent three further screenshots on WhatsApp and these messages showed messages Z had received on Telegram from the Claimant. She says these screenshots demonstrated breaches of the non-molestation order. She exported the screenshots and added them to Z's case file because they were relevant evidential material rather than simply case updates. She goes on to explain she exported the screenshots rather than the whole chat because it was the screenshots that were evidential. She goes on to explain if there had been other messages that met the test for disclosure these would also have been exported and provided as relevant material. She was unable to recall whether there were any such messages as there is no record of them. She goes on to say on 10 July 2024 she also received a TikTok video from Z via email. This was also uploaded to evidence.com and was provided to the Crown Prosecution Service.

24. She says the Claimant was remanded in custody. The allegations of stalking and sexual assault were designated as 'no further action'. She goes on to say she cannot recall whether she had any further communication using WhatsApp as she did not make a record of that when it occurred. However she goes on to say when she receives information that may be relevant or is otherwise important to the case, her usual practice is to create a permanent record of the crime report on the statement so she does not have to rely on memory. She says that the fact that she did not do this for any of her other WhatsApp conversations with Z means that it's likely she did not include anything because she did not consider it to be relevant beyond the conversations and screenshots which she had exported. But she cannot confirm that definitely as she does not have access to the expired messages.

25. She explains that in April 2025 she turned off the disappearing function for all WhatsApp conversations. She explains that any communication she now has with Z takes place via email. She goes on to explain what she calls her reflections on using WhatsApp by the MPS.
26. At the hearing of this matter it became apparent that other information involving DC Archer had not been disclosed. I therefore directed that she file and serve a further witness statement following the hearing, which she duly did so. She explains in a statement that she realised that two further exports of WhatsApp chat with Z in addition to the export on 20 May 2024 had taken place. This was discovered when she checked her email inbox and saw an export from WhatsApp on 27 June 2024 after “chatting” with Z on WhatsApp. A further export after communication with Z then took place in April 2025, before DC Archer switched off the disappearing chat function. She explains the fact she overlooked these later two exports because they all had the same name and so she did not open them when preparing her witness statement for these proceedings and when responding to the defence case statement in the Crown Court proceedings in November 2024. She then goes in to explain how different exports are saved with different types of file names. She states that she downloaded and saved screenshots, images and other media. She explains why there are differences between the exports.

Ground One

27. The Claimant’s first Ground is that the Guidance authorises and approves unlawful conduct by MPS officers and staff. The Claimant’s diffuse skeleton argument states that the Guidance permits unlawful conduct contrary to:
- a. “The CPIA, Statutory Code of Practice and AG Guidelines because it breaches the “requirements to record, retain and reveal material that has “*some bearing on any offence under investigation or any person being investigated or on the surrounding circumstances of the case, unless it is incapable of having any impact on the case*”.
 - b. The DPA, UK GDPR and the COP Code because “data protection by design and default, ensuring that police information can be located, accessed, retrieved

and accurately interpreted, can be trusted as complete and accurate and is subject to periodic review”.

- c. FOIA and the FOIA Code because “retention of information for accountability and audit purposes; destruction policies to adapt to the requirements of litigation, public inquiry, etc; official information on non-corporate communication channels transferred to official systems”.
- d. PRA, IOPC Statutory Guidance and HRA because there is a “duty to obtain and preserve evidence in relation to public complaints, conduct and DSI matters and especially in relation to events engaging the investigative duties under Article 2 and 3 ECHR.”
- e. College of Policing’s Code of Practice on Police Information and Records Management, July 2023 (“the COP Code”) and associated guidance on the Management of Police Information (“MOPI”) because “the requirements of deliberate and purposive retention, quality assurance, audit and reliable access”.

28. I have not found these wide ranging submissions easy to follow. However, paragraph 114 of the Statement of Facts and Grounds is only concerned with CPIA obligations and no other sources of the law. I understood Ms Murphy to accept at the hearing the only alleged misstatement of the law within the Guidance relates to the CPIA obligations, read with the Statutory Code of Practice and the AG Guidelines.

R (A) v Secretary of State for the Home Department

29. The central authority in this regard is *R (A) v Secretary of State for the Home Department* [2021] UKSC 37; [2021] 1 WLR 3931; (“*R (A)*”). The Supreme Court set out the role of the court when considering a policy said to be unlawful at paragraph 41:

“It calls for a comparison of what the relevant law requires and what a policy statement says regarding what a person should do. If the policy directs them to act in a way which contradicts the law it is unlawful. The courts are well placed to make a comparison of normative statements in the law and in the policy, as objectively construed.”

30. Going on to note the three different ways in which a policy might be considered unlawful at paragraphs 46-47:

46. ... (i) where the policy includes a positive statement of law which is wrong and which will induce a person who follows the policy to breach their legal duty in some way (i.e. the type of case under consideration in *Gillick* [1986] AC 112); (ii) where the authority which promulgates the policy does so pursuant to a duty to provide accurate advice about the law but fails to do so, either because of a misstatement of law or because of an omission to explain the legal position; and (iii) where the authority, even though not under a duty to issue a policy, decides to promulgate one and in doing so purports in the policy to provide a full account of the legal position but fails to achieve that, either because of a specific misstatement of the law or because of an omission which has the effect that, read as a whole, the policy presents a misleading picture of the true legal position. In a case of the type described by Rose LJ, where a Secretary of State issues guidance to his or her own staff explaining the legal framework in which they perform their functions, the context is likely to be such as to bring it within category (iii). The audience for the policy would be expected to take direction about the performance of their functions on behalf of their department from the Secretary of State at the head of the department, rather than seeking independent advice of their own. So, read objectively, and depending on the content and form of the policy, it may more readily be interpreted as a comprehensive statement of the relevant legal position and its lawfulness will be assessed on that basis. In the present case, however, the police are independent of the Secretary of State and are well aware (and are reminded by the Guidance) that they have legal duties with which they must comply before making a disclosure and about which, if necessary, they should take legal advice.

31. The Defendant also draws my attention to paragraphs 39 and 40 in support of its defence of the Guidance under this Ground:

“There is often no obligation in public law for an authority to promulgate any policy and there is no obligation, when it does promulgate a policy, for it to take the form of a detailed and comprehensive statement of the law in a particular

area, equivalent to a textbook or the judgment of a court. Since there is no such obligation, there is no basis on which a court can strike down a policy which fails to meet that standard.

...

If the test were more demanding there would be a practical disincentive for public authorities to issue policy statements for fear that they might be drawn into litigation on the basis that they were not sufficiently detailed or comprehensive...the courts would be drawn into reviewing and criticising the drafting of policies to an excessive degree. In effect they would have a revising role thrust upon them requiring them to produce elaborate statements of the law to deal with hypothetical cases which might arise within the scope of a policy. Such a role for the courts cannot be justified.”

32. The Statement of Facts and Grounds accepts “*This is therefore not a case of a positive misstatement of law of the kind within category (i)*” but purports to plead a case based on categories (ii) and (iii). The pleaded case does not properly identify what specific statutory or other law the Guidance is said to misstate or in respect of which there are omissions.

Advice Duty or Full Account?

33. It is not clear from the Statement of Facts and Grounds the source of the duty to provide accurate advice about the law. That is set out in the Claimant’s skeleton argument. The skeleton states the Guidance “*was self-evidently issued pursuant to a legal duty*”. The duty is said to be the following:

“It is the Claimant’s case that in issuing the MPS Policy, the Defendant was exercising statutory powers conferred by section 4(3) of the PRSRA (which places the metropolitan police force and the civilian staff of the metropolitan police force under the direction and control of the Defendant) and paragraph 4(1) of Schedule 4 of the PRSRA which provides that the Defendant “*may do anything which is calculated or is conducive or incidental to, the exercise of the functions of the Commissioner*” but that the Defendant failed to exercise those powers in accordance with the “*policy and objects*” of the statute and took into

account irrelevant considerations while failing to take account of relevant considerations. The policy and objects of the PRSRA include the directing of officers and staff to comply with relevant legal obligations and to promote public confidence in policing. The legal obligations pertinent to police record keeping arise from the CPIA, DPA, FOIA, PRA, HRA and associated Codes of Practice.”

34. It is said the Guidance was issued pursuant to the sub-section 4 (3) PRSRA. Section 4(3) states: “*The metropolitan police force, and the civilian staff of the metropolitan police force, are under the direction and control of the Commissioner of Police of the Metropolis.*” The relevant part of paragraph 4 (4) of Schedule 4 PRSRA that the Claimant appears to rely on states:

(1) The Commissioner of Police of the Metropolis may do anything which is calculated to facilitate, or is conducive or incidental to, the exercise of the functions of the Commissioner.

(2) That includes—

- (a) entering into contracts and other agreements (whether legally binding or not), but only with the consent of the Mayor’s Office for Policing and Crime;
- (b) acquiring and disposing of property, apart from land, but only with the consent of the Mayor’s Office for Policing and Crime.

35. I agree with the Defendant’s submission that nowhere has the Claimant articulated a *Re A* limb (ii) advice duty. I agree with the Defendant, that section 4 (3) and paragraph 4 of schedule 4 of PRSRA do not establish an advice duty. It follows that there can be no breach of limb ii of *Re A*.

36. Nor has the Claimant succeeded on demonstrating a breach of limb (iii) of *Re A*. It is self-evidently the case the Guidance is concerned with managing use of instant messaging. It is not attempting to explain CPIA obligations to MPS officers. Therefore the requirement in *Re A* that the Defendant “purports in the policy to provide a full account of the legal position” is unarguable.

37. Given the Claimant cannot establish an Advice Duty (*Re A* (ii)) or an attempt at providing a full account of the law (*Re A* (iii)) it is unsurprising the Claimant's Grounds and skeleton both fail to set out the comparison between what the law requires (and where this is stated in the law) and, by comparison, where the Guidance is said to be erroneous cross-referenced to the law.
38. For these reasons Ground One fails. But given the importance of the issue and given the overlap with Ground Three, it is necessary to go on to consider whether the Guidance does misstate the law. If it did this could have serious consequences.

CPIA Obligations

39. That aside, does the Guidance contravene the CPIA obligations? Ms Murphy relied on Part 1 CPIA provisions such as section 3 and 7A. I agree with Ms Idelbi that these obligations relate to prosecutors and not the police – see the heading to section 3 “Initial Duty of Prosecutor To Disclose” and the various references to “prosecutor”. Likewise section 7A is clearly directed at prosecutors and not the police. Ms Idelbi was correct to take me to Part 2 of the CPIA as Part 1 deals with persons who have been charged (see section 1 (1) CPIA).
40. Section 23 is within Part II of the CPIA entitled “Criminal Investigations”. Section 23 (1) states: that the “*Secretary of State shall prepare a code of practice containing provisions designed to secure*”, among other things (my emphasis added)—
- “(b) that information which is obtained in the course of a criminal investigation and may be relevant to the investigation is recorded;
- (c) that any record of such information is retained;
- (d) that any other material which is obtained in the course of a criminal investigation and may be relevant to the investigation is retained.”
41. As I understand the statutory scheme the CPIA does not create statutory duties on police forces, rather there is a duty on the Secretary of State to prepare a Code of Practice.

42. The ‘Revised CPIA Code of Practice’ (hereafter “the Code”) sets out the definition of the ‘material’ to be secured at paragraph 2 as “*material may be relevant to an investigation if it appears to an investigator, or to the officer in charge of an investigation, or to the disclosure officer, that it has some bearing on any offence under investigation or any person being investigated, or on the surrounding circumstances of the case, unless it is incapable of having any impact on the case.*”

43. The Code, in Section 5 on retention, states:

- a. “5.1 The investigator must retain material obtained in a criminal investigation which may be relevant to the investigation.”
- b. “5.3 If the officer in charge of an investigation becomes aware as a result of developments in the case that material previously examined but not retained (because it was not thought to be relevant) may now be relevant to the investigation, he should, wherever practicable, take steps to obtain it or ensure that it is retained for further inspection or for production in court if required.”

—

- c. ¶5.4 focuses on material that “*may be relevant*” and states:
“The duty to retain material includes in particular the duty to retain material falling into the following categories, where it may be relevant to the investigation: crime reports (including crime report forms, relevant parts of incident report books or police officers’ notebooks);
 - custody records;
 - records which are derived from tapes of telephone messages (for example, 999 calls) containing descriptions of an alleged offence or offender;
 - final versions of witness statements (and draft versions where their content differs from the final version), including any exhibits mentioned (unless these have been returned to their owner on the understanding that they will be produced in court if required);
 - interview records (written records, or audio or video tapes, of interviews with actual or potential witnesses or suspects);
 - communications between the police and experts such as forensic scientists, reports of work carried out by experts, and schedules of scientific material

prepared by the expert for the investigator, for the purposes of criminal proceedings;

- records of the first description of a suspect by each potential witness who purports to identify or describe the suspect, whether or not the description differs from that of subsequent descriptions by that or other witnesses;
 - any material casting doubt on the reliability of a witness.”
- d. “5.6 *The duty to retain material falling into these categories [i.e. in Code ¶5.4] does not extend to items which are purely ancillary to such material and possess no independent significance (for example, duplicate copies of records or reports).*”

44. In respect of recording of information, Section 4 explains:

“4.1 If material which may be relevant to the investigation consists of information which is not recorded in any form, the officer in charge of an investigation must ensure that it is recorded in a durable or retrievable form (whether in writing, on video or audio tape, or on computer disk).

4.2 Where it is not practicable to retain the initial record of information because it forms part of a larger record which is to be destroyed, its contents should be transferred as a true record to a durable and more easily-stored form before that happens.

...

4.4 Where information which may be relevant is obtained, it must be recorded at the time it is obtained or as soon as practicable after that time. This includes, for example, information obtained in house-to-house enquiries, although the requirement to record information promptly does not require an investigator to take a statement from a potential witness where it would not otherwise be taken.”

45. The ‘Attorney General’s Guidelines on Disclosure for investigators, prosecutors and defence practitioners on the application of the disclosure regime’ (hereafter the “AG Guidelines”) “*outline[s] the high-level principles which should be followed when the disclosure regime is applied throughout England and Wales. They are not designed to*

be an unequivocal statement of the law at any one time, nor are they a substitute for a thorough understanding of the relevant legislation, codes of practice, case law and procedure.”

46. Paragraph 23 states:

“It may become apparent to an investigator that some material obtained in the course of an investigation, either because it was considered to be potentially relevant, or because it was inextricably linked to material that was relevant, is in fact incapable of impacting on the case. It is not necessary to retain such material. However, the investigator should also exercise considerable caution in reaching that conclusion. The investigator should be particularly mindful of the fact that some investigations continue over some time. Material that is incapable of impact may change over time and it may not be possible to foresee what the issues in the case will be. The advice of the prosecutor may be sought where necessary. Ultimately, however, the decision on whether to retain material is one for the investigator, and should always be based on their assessment of the relevance of the material and the likelihood of it having any impact on the case in future.”

47. Annex A states at paragraph 1:

“This annex is intended to supplement the Attorney General’s Guidelines on Disclosure. It is not intended to be a detailed operational guide but is intended to set out a common approach to be adopted when seeking to obtain and handle digital material, whether that be from a suspect or from a complainant or witness.”

48. Further, it states at paragraph 6 (a): *“No action should be taken which changes data on a device which may subsequently be relied upon in court.”*

Claimant's Case on Breach of CPIA Obligations

49. The Statement of Facts and Grounds pleads the unlawfulness against the CPIA obligations in this way:

- a. it permits deletion of communication with suspects;
- b. it places undue weight on evidential material over (non-evidential) relevant material;
- c. it fails to identify the true legal status of the communication;
- d. it fails to identify the place of such communication in the ongoing disclosure process;
- e. it provides for insufficient safeguards;
- f. it is in breach of the AG's Guidelines, which require no changes to be made to data on devices.

50. The high water mark of the Claimant's case in the skeleton argument is that:

“...the MPS mandates officers to activate disappearing messages with the effect that information that *may* be relevant to an investigation will not be retained (in contravention of section 23(1) of the CPIA). The test of whether information *may* be relevant is exceptionally broad and includes information that has “some bearing on any offence under investigation or any person being investigated, or on the surrounding circumstances of the case, unless it is incapable of having any impact on the case” (SOFG [CB/42, §67]). In this sense the MPS Policy mandates unlawful conduct: the destruction of material that ought to be retained for CPIA review and potential disclosure.”

51. The reference above is to paragraph 2.1 of the CPIA Code. However, it is important to add in the words which precede it: “material may be relevant to an investigation if it appears to an investigator, or to the officer in charge of an investigation, or to the disclosure officer, that it has...” (my emphasis added).

52. In attempting to articulate why the Guidance misstates the law, the Claimant's skeleton and oral submissions make a number of further points:

- a. The Guidance unlawfully requires the deletion of communication with suspects “*for a policing purpose*”.
- b. The Guidance unlawfully restricts retention of material to “*evidential*” material, but omits “*relevant*” or “*disclosable*” material.
- c. the AG’s Guidelines makes plain (i) “*inextricably linked non-relevant material which it is not reasonably practicable to separate can also be retained*”; and (ii) “*[m]aterial which is inextricably linked to relevant unused material which of itself may not be relevant material ... should be retained*”
- d. the point is made that at ninety days the relevance of material will often not be known but will be automatically deleted.

53. I have not set out all the Claimant’s arguments under this submission on Ground One as plainly many of them do not relate to the issue of the misstatement of law, but rather deal with *the risk* of the Guidance being applied or misapplied by individual MPS officers leading to a breach of the CPIA obligations. Lord Sales and Lord Burnett reject such a ground of challenge against a policy based on the risk of illegality for the comprehensive reasons set out in paragraph 65. As was stated: “*If one simply asks whether a policy creates an unacceptable risk that an individual will be treated unfairly (which is to say, unlawfully), there is a danger that this could be taken as a freestanding principle distinct from that in Gillick¹.*”

Does the Guidance Misstate the CPIA Obligations?

54. The CPIA itself does not require police forces to retain information. Plainly the Code and the Attorney General’s Guidelines do. This is for obvious reasons.

55. I accept the points made by the Defendant about the Guidance which must be considered in the context of the Supreme Court’s learning at paragraph 65 of *Re A* where it was held that the test for lawfulness of the policy was based on “what is stated to be the behaviour required if the policy is followed”. Should MPS officers and staff properly follow the Guidance, then the following should be the position:

¹ Re A at paragraph 64.

- a. officers and staff are required to comply with the wider MPS policies regarding the use of MPS systems;
- b. officers and staff must comply with their professional responsibilities and behaviour standards;
- c. officers and staff are not required to use WhatsApp but rather they are invited to consider the most appropriate mode of communication;
- d. officers and staff are prohibited from using WhatsApp for communicating sensitive information, confidential or evidential material, or material generated in the course of an investigation which would engage CPIA retention and disclosure obligations, or operational decision making;
- e. officers and staff are required to export and retain WhatsApp conversations if a prohibited use occurs and the Guidance explains to officers and staff how that can be done.

56. I also accept the point made by the Defendant that it is for individual police officers to use judgement and assess what is relevant or irrelevant material. The Guidance must be seen in this context.

57. The Claimant is correct to be concerned that the automatic delete function at ninety days will lead to information being deleted. But it is not a statement of the law. The Guidance does not misstate the law in this regard. The Guidance does not compel officers to use instant messaging or WhatsApp. It requires officers to not use instant messaging for “*Evidential material, or material generated in the course of an investigation which would engage CPIA retention and disclosure obligations – this would include significant updates on an investigation to victims of crime.*” The Guidance directs officers to use instant messaging to support the functioning of the workplace and work relationships and states it is not a “*forum to create, share, record or store operational information.*” The Guidance notes that should evidential material be sent unexpectedly then: “*then the chat can be exported (see guidance in annex 1) and uploaded to Axon Capture, by the user, as soon as possible and all actions properly recorded on Connect.*” Therefore if an officer chooses to use WhatsApp and communicates with a suspect, the Guidance does not misstate the law in regard to CPIA obligations. The Guidance directs MPS officers to their CPIA obligations.

58. The Claimant complains that the Guidance misstates the law for three inter-related reasons: (i) it places undue weight on evidential material over (non-evidential) relevant material; (ii) it fails to identify the true legal status of the communications and (iii) it fails to identify the place of such communication in the ongoing disclosure process. I do not find any of these points result in the Guidance misstating the law. The Guidance is about instant messaging not a complete statement of the CPIA obligations. This point is bound up with why this ground fails the *Re A* limb (iii) as it is not attempting to state CPIA obligations.
59. The Claimant may consider further safeguards are required. But that does not result in the Guidance misstating the law.
60. Lastly there is one specific identification of a purported breach of the CPIA obligations which is the reference to paragraph 6 (a) of Annex A of the Attorney General's Guidelines, but it seems to me the Defendant is correct to submit this Guidance relates to the handling of a device that is being examined for evidential value, not a police issued device.
61. I understand the Claimant's anxiety about an officer knowing or envisaging the relevance of material when it is received and within the ninety days before it is deleted and that its relevance may not be known. Clearly caution is required and officers should be proactive in exporting any material which might be relevant. But again this does not involve a misstatement of the law.
62. I note the use of the word "can" in the last sentence of the Guidance before the summary: "*If this occurs then the chat can be exported (see guidance in annex 1) and uploaded to Axon Capture, by the user, as soon as possible and all actions properly recorded on Connect.*" 'Can' should properly be replaced with "should" but I am satisfied reading the Guidance as a whole that MPS officers and staff realise the necessity of preserving CPIA or evidential material through export, should it be unexpectedly sent to them.
63. For these reasons Ground One fails.

Ground Two

64. *Padfield v Minister of Agriculture, Fisheries and Food* [1968] AC 997 (“Padfield”) concerned the refusal of the Minister to appoint a committee of investigation to resolve a dispute on the differential for the payment of milk produced in different regions in England and Wales. The Agricultural Marketing Act 1958 conferred the discretion to appoint, and so the access to, a committee of investigation on the Minister, which was the only appropriate remedy for resolution of the dispute (at 1027C-D). Lord Reid explained at 1030B-D that:

“Parliament must have conferred the discretion with the intention that it should be used to promote the policy and objects of the Act; the policy and objects of the Act must be determined by construing the Act as a whole...if the Minister...so uses his discretion as to thwart or run counter to the policy and objects of the Act, then our law would be very defective if persons aggrieved were not entitled to the protection of the court.”

65. The Claimant’s pleaded case states that the Guidance is *Padfield* improper having regard to the CPIA, “the DPA, the FOIA, PRA and HRA”. The pleadings do not identify the statutory discretions said to be thwarted by the Guidance.

66. The Claimant’s skeleton argument refined his submission to submit that the Guidance was “issued” pursuant to PRSRA. The skeleton argument does not clearly explain what the power/discretion is, which results in the Guidance being *Padfield* improper. I think it is being suggested the power is the power to direct and control the Metropolitan Police. The skeleton argument does not set out how the Guidance frustrates the purpose of the PRSRA generally or specifically, alternatively nor does it set out the Guidance furthers an alternative purpose, that Parliament did not intend.

67. I agree with the Defendant that the PRSRA does not confer a discretion on the Defendant to issue the Guidance. PRSRA is concerned with the structural organisation of the Defendant and its legal personality.

68. A *Padfield* challenge cannot succeed.

69. The Claimant appears to make a further submission to expand the *Padfield* duty beyond discretionary powers conferred by Parliament and/or to decisions and policies that arise outside a contained statutory framework, such that any policy inconsistent with the intention of any Act of Parliament would be unlawful. This submission is untenable. Sir Nicholas Underhill (with the agreement of Baker and Elisabeth Laing LJ) in *R((Refugee and Migrant Forum of Essex and London and another) v Secretary of State for the Home Department (No. 1)* [2025] EWCA Civ 1843; [2026] 1 WLR 1478 (at paragraph 72) rejected a similar submission, noting that:

“It is obvious that a public body cannot exercise any of its powers in a way which is contrary to other legislative provisions; but that is not because of the *Padfield* principle, which is, as Cavanagh J demonstrates by reference to the authorities, altogether narrower. I note that *Padfield* was not even cited to the court in the *New London College* case. No doubt at a very deep level the two limitations are underpinned by the same principle, namely that a public body must always act within the powers that Parliament intended it to enjoy...”

70. Ground Two is dismissed.

Ground Three

The Claimant Case on Unreasonableness of the Guidance

71. It is important to emphasise that the Claimant challenges the specific part of the Guidance which requires the automatic deletion at ninety days without a reliable mechanism for retention and storage. Very little was submitted about the reliability of Connect once messages are uploaded. The *Wednesbury* challenge is not to the decision to permit WhatsApp or other instant messaging applications on MPS devices.

72. To make good the assertion of *Wednesbury* unreasonableness the Claimant relies on a number of reports. The Claimant relies on a September 2019 report from HM Inspectorate of Constabulary and Fire and Rescue Services entitled “PEEL Spotlight

Report – Shining a Light on Betrayal.” This report dealt with abuse of trust within forces for sexual purposes and looked at how officers communicated with each other. The report states:

“Forces that don’t monitor the sensitive information officers and staff are viewing on force mobile phones create an exceptionally high risk for themselves. The use of encrypted apps can make monitoring harder. Forces need to reassure themselves that they understand all the risks of having encrypted apps on force-issue phones. They then need to take steps to mitigate those risks.”

73. The Claimant relies on the 2019 Independent Office for Police Conduct (“IOPC”) ‘Operation Argens’ Report concerning an investigation into allegations of discriminatory and inappropriate comments made by MPS officers within a WhatsApp group chat between March and October 2019. This report raises serious issues of police misconduct when communicating on WhatsApp.
74. The Claimant makes reference to the May 2018 National Police Information Risk Management Team paper entitled “Use of WhatsApp and other Social Networking Applications, Principles of Use.” Annex A of this report states that from a policing perspective, personnel are strongly advised not to use WhatsApp to exchange police information.
75. The Claimant’s pleaded case also relies on the caution about WhatsApp use contained in the IOPC report “Independent Review into the use of WhatsApp and other instant messaging applications within the police service” published in 2024. This report flags disclosure and data protection issues. The Claimant relies on this passage in particular:

“Fulfilling information related obligations where WhatsApp is used for police work. Police forces have legal obligations for information collation and storage. WhatsApp is not a police system and is not connected to police systems. WhatsApp chats may form a part of a police investigation file, which would require a process by which chats can be saved to the relevant file: an audit trail of relevant information. There are also legal obligations for accessibility, disclosure, processing and retention. The information obtained during this

review suggests police forces need to put in place processes to ensure they fulfil these obligations.”

76. Reference is also made to the Information Commissioner’s Office’s Guidance on the Freedom of Information Act 2000. The pleaded case states: “The ICO identified the risks arising from auto-deletion and stated: “*As far as reasonably practicable, you should always ensure that you use corporate channels for official business. Where this is not possible for whatever reason, you should make arrangements to store official information on your corporate systems as quickly as possible*”. Further, that such transfer should be undertaken “frequently and routinely” so as to minimise information loss and the burden falling on individuals to consider what information ought to be retained, and ensure that auto-delete options should be in line with retention policies.”

77. The National Police Chief Council (“NPCC”) issued a report on 9 January 2023 which the Claimant submits discourages the use of WhatsApp for policing purposes. This document states the following:

“Whilst it is recognised that there are significant benefits in the use of instant messaging. The use of WhatsApp for policing purposes, presents an information security risk with data being managed outside of the United Kingdom and the police service having no jurisdiction on the control of that data. You will also be aware of the CPIA implications to consider with the retention of relevant material stored within encrypted applications.

....

In the interim to mitigate the risks associated with encrypted applications, we would encourage the use of the Microsoft O365 Teams Chat and TeamSpace functions which is auditable and replicates the functionality of WhatsApp.”

78. A DPIA was carried out by the Defendant in March 2023 on the issue of deploying WhatsApp to MPS devices. The Claimant characterises this document as identifying “high” risks. This document identifies the MPS as the “controller” and Meta as the “processor” to use Data Protection Act 2018 language. This report acknowledges “WhatsApp presents a number of well understood security risks.” It states any MPS

policy would need to understand the risks. It states that law enforcement processing should not be “transacted via WhatsApp.” It states:

“WhatsApp is a widely used app by a number of members of the public. The MPS requires to use the app to ensure that we can communicate with all members of our communities. It is also required to ensure MPS colleagues can use it to engage with each other and prevent them from using it on their personal devices for work purposes. If WhatsApp is used in line with our proposed use, it is not foreseen that there will be a high level of risk in relation to the sharing of any MPS data.”

79. The DPIA was updated on 17 August 2023 after receipt from the Information Commissioner dated 18 July 2023. Paragraph 40 of the updated DPIA states:

“This updated draft DPIA seeks to respond to the ICOs helpful commentary and is updated with changes to the planned operation model. Significantly, it was originally envisaged that LBM might capture routine incoming and outgoing WhatsApp traffic and in effect produce a central ‘data lake’ which could be interrogated to deal with rights of access under both DPA18 and FOIA2000 legislative provisions. However whilst nothing escapes the purview of LBM there will be no comprehensive recording of all messages i.e. no comprehensive central record. On the basis of sensitivity, the operating model for LBM will not be detailed herein but will be confined to the relevant LBM DPIA”

80. Paragraphs 57 and 58 deal with retention and deletion of WhatsApp messages and states:

“WhatsApp messages are stored on the end user’s device rather than in any corporate repository which is centrally located. WhatsApp may also be configured to back up the messages to cloud storage. The issues of retention, review, and deletion and ensuring that records find their way into the appropriate repository are significant. For example, the MPS would not be able to comply with a data subject statutory rights unless it can ascertain whether personal data relating to the individual exists. The same is true in respect of

whether the MPS holds information related to a particular subject unless likewise this can be searched for.

It is therefore recommended that the MPS ensures that:

- ☐ A base retention period is set by the MPS to meet business need and to curtail excessive retention.
- ☐ That there is a mechanism in place which ensures that messages reaching end of life are automatically deleted unless there is a reason for further retention and that deletion is from devices and any backups.
- ☐ A mechanism is developed to deliver a capability of comprehensive central searching of WhatsApp messages at least (but not exhaustively) by topic, dates, MPS sender/recipient, and personal information held. This will enable core rights and obligations to be upheld. These include DPA 18 rights of access and rights to be forgotten etc.; FOIA 2000; Public Inquiries Act 2005; etc.
- ☐ That mechanisms and policies are reviewed to ensure that material which should be transferred into some other form of corporate storage for the purposes are identified and transferred. For example that intelligence is moved into the intelligence system and records relevant to CPIA is moved into case files.”

81. The DPIA states at paragraph 67:

“At this stage of development and without sight of scope and policy in respect of usage; and of mitigations to risk, it is impossible to adequately assess residual risk. As such the residual risks to the rights and freedoms of individuals must be assumed to remain high. This DPIA should therefore be further developed to the extent that the processing risks and mitigations can be fully described and reviewed again at that point. Mandatory referral to the ICO is only required before processing commences where risks cannot be mitigated below high.”

82. The email from the Information Commissioner responds to the Defendant’s concerns about the international transfer of data noting “there is a limited need to consider the questions around international transfers.” The email goes on to raise these issues:

“We do have some other questions around the DPIA, however, and I’d like to raise these here for your consideration and response when appropriate:

Paragraph 19 – what form will the Lawful Business Monitoring take? How is this done via individual devices and will this require that the WhatsApp messages are copied to, and retained on, other MPS systems? If so, what access controls and governance will secure that information? Is there any risk of collateral intrusion into messages received from the public, eg are these stored in MPS servers somewhere?

Para 23 – esp deletion. I note the messages are intended to auto-delete at 90 days, and transferred to other police systems if retention is required. What mechanism will the MPS put in place to respond to a deletion request received within the 90 day period? Similarly, what measures will control how a subject access or FOI information request is responded to if received within the 90 day period? See also para 26 and 27 re retention under Lawful Business Monitoring – what measures will be in place to give effect to individuals’ rights, and the right of access under FOIA?”

83. The Information Commissioner’s email further states:

“As you have detailed, the use of WhatsApp within MPS should be accompanied by clear policies to manage the associated risks, especially regarding external groups and the potential lack of oversight. Staff should exercise caution while using WhatsApp due to its known security vulnerabilities, such as the minimal requirements for registration and user identification. Just to further highlight the importance that sharing of personal data on the platform should be limited, WhatsApp use should primarily focus on administrative and logistical purposes. We would recommend that internal guidance is very clear and explicit as to the limits of acceptable use.”

84. Ms Murphy also relied on an email dated 14 July 2023 where it was noted an official from the Information Commissioner’s Office gave evidence to the House of Commons

Public Administration and Constitutional Affairs Committee and the author was of the view from watching this the ICO was “vehemently opposed to the use of disappearing messages”.

85. The Claimant also relies on the Defendant’s own evidence in respect of the development of the Guidance. The following key points are made in the skeleton argument:

- a. There was encouragement at a senior level to roll out WhatsApp to officers because of its ease of communication with members of the public;
- b. At an early stage Mr Scates identified that WhatsApp was not “Management of Police Information – (“MOPI”) or DPA compliant as it did not have a central search function, but this could be addressed by an LBM functionality;
- c. Mr Scates produced a further paper on 16 January 2023 reiterating that WhatsApp was not MOPI or DPA compliant but that LBM would seek to deal with this;
- d. On 10 February 2023 the Defendant’s SLT noted the 9 January 2023 NPCC advice and further noted Mr Scates’ paper that LBM technology would be available from March 2023 and that WhatsApp on MPS devices presented less risks than on personal devices;
- e. The DPIA purportedly showed “high” risks and envisaged a comprehensive central searching function;
- f. The ICO views were sought in June 2023 and the DPIA was further updated;
- g. On 4 August 2023 the decision was made to roll out WhatsApp on MPS devices from 1 September 2023 and Mr Scates was to address outstanding issues although the Claimant’s skeleton is not clear what those issues were;
- h. A survey of 24 October 2023 noted that not all MPS officers were aware of the Guidance and that WhatsApp was used contrary to the Guidance;
- i. The original plan to implement WhatsApp on MPS devices was for there to be a LBM with a central retained searchable database, which the Claimant submits was essential for CPIA compliance, but the policy was pushed forward despite there being no retained central database which could be searched.

86. The Claimant then makes four points on the unreasonableness:

- a. “the Defendant gave undue weight to the speculative possibility that there would be advantages in terms of public engagement through reliance upon WhatsApp and insufficient weight to the contrary position that encouraging 1:1 communication (rather than team responsibility) would undermine the public’s confidence;
- b. the Defendant’s consideration that the introduction of WhatsApp on MPS issued devices would reduce officers’ reliance upon WhatsApp on their personal devices militated against the introduction of a WhatsApp strategy that was entirely dependent on policy controls to secure statutory and regulatory compliance; if the Defendant lacked confidence in his officers’ compliance in one area of WhatsApp usage he ought not to have had confidence in their compliance in another.
- c. it was irrational to persist in the WhatsApp roll out in the face of significant opposition from informed external bodies including the NPCC, IOPC and ICO especially after the anticipated LBM functionality did not materialise;
- d. it was irrational for the Defendant to insist on the roll out in the face of Mr Scates’ papers of November 2022 **and** 16 January 2023, Mr Harman’s update of August 2023 and especially after it became apparent the LBM could not in fact achieve a central searchable database of the communications.”

87. The Claimant also made post-hearing submissions on this ground in the light of DC Archer’s second witness statement. Ms Murphy submitted:

“Further, DC Archer’s described practice in relation to her WhatsApp communications with the complainant, her practice in relation to “chat” exports and her practices in relation to saving media (i.e. material sent in addition to “chat” content) underline the Claimant’s case that the Commissioner’s Policy on WhatsApp and instant messaging (“the MPS Policy”), especially those elements that (i) mandate reliance upon disappearing messages, (ii) permit interaction with complainants/witnesses/suspects and (iii) propose a means for evidential export, is incapable of ensuring sufficient compliance with the CPIA regime. The MPS Policy is therefore unreasonable and unlawful.”

The Defendant's Response

88. Ms Idelbi emphasised that the DPIA was carried out in relation to the deployment decision to roll out WhatsApp on MPS devices and it is not a DPIA in respect of the ninety day deletion policy. She makes the submission that nearly all the reports and advice relied on by the Claimant were considered by the Defendant as it developed the Guidance. She relied in particular on paragraphs 18 to 20 of Chief Inspector Peter Shaw's witness statement where he lists documents he took into account and others he recalls might have been considered. Therefore Ms Idelbi points out that those responsible for the Guidance have considered the documents the Claimant relies on in his *Wednesbury* challenge.

89. The Defendant argues that most of the Claimant's case relates to the decision to deploy WhatsApp on MPS devices and notes this is not the subject of challenge. The Defendant submits the Claimant's Grounds and Skeleton mischaracterise or selectively quote from the various reports relied on in the Statement of Facts and Grounds. The Defendant submits the DPIA carefully evolved after consultation with stakeholders including taking into account and responding to the Information Commissioner's July 2023 email. It was also submitted that the Claimant's case is predicated on WhatsApp and the Guidance being deployed without any risk. The Defendant submits it is not possible for a police force to eradicate all risks and there is much risk mitigation in place. The Defendant also makes clear the Claimant has not shown why no reasonable police commissioner would have opted for ninety day retention as opposed to: twenty four hours; seven days or indefinite retention.

90. The Defendant also submits "*It would be inconsistent for a policy to be lawful by analysis under Gillick but for the analysis under Wednesbury to render the same policy unlawful on the same premise.*" This appears to be a submission related to the need to assume compliance with the policy under challenge.

91. Ms Idelbi also submitted the Guidance was consistent with the principles of the DPA and the FOIA, making the point that the latter does not impose an obligation to retain information generally. She also stressed the fact the Guidance must be seen in its proper context and there is a suite of MPS policies that must also be applied.

92. It was emphasised by the Defendant that there are always risks to material being lost. Notebooks can be lost. Emails can be incorrectly deleted. “Bodycam” footage is not downloaded. On the other hand it was also pointed out that there are risks with indefinite retention of WhatsApp chat messages which makes it less likely officers would proactively upload the information.

93. Following the post-hearing evidence and submissions, the Defendant submitted that:

“A system does not fail the rationality test simply because its design or day-to-day operation is capable of improvement in some respects, RAMFEL at [67] [SAB/1374 (pdf 1378)]. A system does not become unlawful because it creates an unacceptable risk that an individual would be treated unlawfully, A v SSHD at [65C-D] [CAB/191]. Those are the high hurdles. The Claimant’s example of one is incapable of surmounting that high hurdle.”

Analysis

94. I agree with the Defendant that from a ‘process rationality’ perspective, nearly all of the items and papers and reports raised by the Claimant are all matters which have been considered by the Defendant’s witnesses as their witness statements explain. I note the Claimant does not submit there has been any breach of his rights pursuant to the DPA or the FOIA. It is also the case that the Defendant carefully considered the context of rolling out WhatsApp to MPS devices over a period of time and carried out consultation with stakeholders in respect of this process. Whilst much criticism is made of the email from the Information Commissioner, it seems sensible for the Defendant to have engaged with the Information Commissioner and sought views on the DPIA. The DPIA was amended to reflect the engagement with the Information Commissioner. This was not required but was good practice.

95. I find that the Guidance reflects much of the advice contained in the reports relied on by the Claimant. It is clear from the “General Principles of Use” section that LBM applies to instant messaging including WhatsApp. The Defendant’s witness statement support this. The Guidance instructs officers not to use WhatsApp for evidential

material or material generated in an investigation which would engage CPIA obligations. WhatsApp or other instant messaging is there to be used for short term disposable communication. This is very much in line with some of the critique produced in the reports relied on by the Claimant. Indeed the main thrust of the Information Commissioner's advice, which I repeat, is reflected in the Guidance:

“As you have detailed, the use of WhatsApp within MPS should be accompanied by clear policies to manage the associated risks, especially regarding external groups and the potential lack of oversight. Staff should exercise caution while using WhatsApp due to its known security vulnerabilities, such as the minimal requirements for registration and user identification. Just to further highlight the importance that sharing of personal data on the platform should be limited, WhatsApp use should primarily focus on administrative and logistical purposes. We would recommend that internal guidance is very clear and explicit as to the limits of acceptable use.”

96. The Defendant is correct to observe that much of the evidence of *Wednesbury* unreasonableness relates to the decision to deploy WhatsApp and not the ninety day automatic deletion policy/storage. Very little is said by the Claimant about that specific issue. Very little is said in the various reports that the Claimant seeks to rely on to make good his submission on this ground. Ms Murphy accepted there could not be indefinite retention of WhatsApp ‘chat’ data. The Claimant does not properly explain why it was unreasonable for the Defendant to rely on the ninety day automatic delete function as opposed to a different unidentified period. Given the valid concerns raised by the Claimant about the need to secure CPIA material, it seems obvious that the twenty four hour and seven day automatic delete options make less sense. The Commissioner has crafted a scheme to preserve CPIA or other evidential material and considers deletion of other messages rather than indefinite retention is the best design for his officers and staff. No particular complaint was made about Connect storage.

97. Although the Guidance and the deployment of WhatsApp took place in September 2023, the Claimant has not identified other cases or any reported appellate cases of the Guidance leading to difficulties in the criminal justice system. The Defendant, with its

duty of candour, has provided no document or information which evidences the type of widespread problems that the Claimant submits exist with CPIA obligations and LBM monitoring. This seems relevant to any *Wednesbury* challenge, although I note the complaints made by the Claimant about the Defendant's compliance with the duty of candour. Whilst DC Archer's second witness statement causes some concern, it is not correct to assume without further evidence that there are widespread issues.

98. The Defendant's evidence in respect of App X explains how LBM works even though there is no central searchable database. I accept DS Millyard' evidence about the approach to risk based monitoring and the evolution from an LBM with a searchable data base. This appears a technical issue of how LBM is deployed. The Claimant has not succeeded in demonstrating any infringement of his statutory rights in respect of LBM, the DPA or the FOIA.
99. Ultimately, it is the judgement of the Defendant that permitting MPS officers and staff to use WhatsApp on MPS devices, with the ninety day automatic deletion function, strikes the correct balance for law enforcement purposes in his area of responsibility. It is for the Defendant to assess the benefits of increased communication with others of instant messaging. In the first place it is for the Defendant to assess the risks of the Guidance and he accepts there are risks. This is an application for judicial review and the Commissioner has the responsibility to assess the benefits, dis-benefits and risks of the Guidance. Under this Ground the court can only intervene if no reasonable police commissioner would rely on the ninety day delete function in WhatsApp with Connect storage of the material identified in the Guidance. I cannot conclude the Claimant reaches this high threshold. Whilst I have reservations about deleting potentially relevant material in the context of criminal proceedings where liberty is very often at issue, and whilst I recognise the importance of maintaining high standards of fairness to ensure compliance with CPIA obligations, the Guidance, seen overall, directs officers to use WhatsApp in a limited way and through uploading any investigation and/or CPIA material to Connect, it provides a mechanism to ensure compliance with CPIA obligations.
100. I dismiss this ground of challenge.

Ground Four

101. The Claimant's pleaded case is that the Guidance "violates article 6 of the ECHR ...and common law entitlements to a fair trial." It is said that by virtue of the Guidance suspects and defendants are "at a significant risk of evidence and exculpatory material in their cases being deleted, which would violate Article 6 (3) (b)" ECHR. Reference is made to *Natunen v Finland App* (2009) 49 E.H.R.R. 32. It is said that the application of the Guidance to the Claimant in the Crown Court proceedings is likely to have resulted in deletion of evidence and relevant material.

102. In *Natunen* the applicant complained pursuant to Articles 6(1) and (3)(b) ECHR that the criminal proceedings had been unfair. He complained that the destruction of a major part of the recordings by the police had not been in conformity with the principle of equality of arms and had deprived him of the right to have adequate facilities for the preparation of his defence. The recordings were telephone records of covert communications between co-conspirators, in circumstances where the prosecution's case relied on joint enterprise. Further the prosecutor accepted that the deleted material was potentially relevant. The court held at paragraph 43:

"Failure to disclose to the defence material evidence, which contains such particulars which could enable the accused to exonerate himself or have his sentence reduced would constitute a refusal of facilities necessary for the preparation of the defence, and therefore a violation of the right guaranteed in art.6(3)(b) of the Convention."

103. The Court found a violation of Article 6 (1) taken together with 6 (3) (b) because:

"The Court recalls that, in this case, the decision regarding the undisclosed evidence was, presumably, made in the course of the pre-trial investigation without providing the defence with the opportunity to participate in the decision-making process. In the present case the Court further notes that the contested measure stemmed from a defect in the legislation, in that it failed to offer adequate protection to the defence, rather than any misconduct of the authorities, who were obliged by law, in force at the time, to destroy the impugned recordings. The Court

observes that in the Government Bill for the amendment of the Coercive Measures Act it was considered problematic that information supporting the innocence of the suspect could be destroyed before the resolution of the case.”

104. The Claimant states that in the light of *Natunen* the existence of the Guidance amounts to a violation of his Article 6 rights. I cannot accept that submission. The principle set out in *Natunen* is factually far removed from the facts of the prosecution of the Claimant.

105. The Claimant made limited reference to Ground Four in his counsels’ written submissions post hearing (paragraphs 9 and 12). It is not clear to me whether the Claimant is submitting that any of the original or later discovered material exported to Connect by DC Archer is said to be relevant or exculpatory. Nor is it clear whether the Claimant accepts the material is not relevant. Ms Idelbi appears correct to point out that: “*The Claimant has not pointed to any part of the chat itself that was relevant material.*” Furthermore, I also agree that it is not clear what material the Claimant does or does not have and it is not clear what was disclosed and when. The Defendants is right to point out that the CPS is not present to answer disclosure queries. I record that it is concerning that it took these proceedings to prompt DC Archer to re-assess whether there was further exported material from WhatsApp communications with Z. I further note it is concerning that this information may not have come to light prior to the earlier scheduled trial in the Crown Court, but I also recognise I am not clear what has been disclosed to the Claimant when and he has not filed a witness statement in these proceedings.

106. I cannot accept the submission that the existence of Guidance or its application violates any of the Claimant’s Article 6 rights to a fair trial or infringes his common law rights to a fair hearing. The significance of the non-disclosure of the material – whether it is relevant or irrelevant – is a matter for the Crown Court proceedings. It will be open to the Claimant to have his counsel cross-examine DC Archer in the Crown Court. If there has been an unfairness or a violation of protected ECHR rights, then these submissions can be made in the Crown Court. It is open to the Claimant to make an application there has been an abuse of process. Article 6 ECHR obligations must be

assessed holistically in the context of the Crown Court proceedings, any cross-examination and any applications made within those proceedings. Sitting in the Administrative Court, I do not have the papers from the prosecution of the Claimant in the Crown Court proceedings and nor is the Crown Prosecution Service a party to these proceedings. In all these circumstances the issue of whether there has been a violation of Article 6 ECHR or common law rights is a matter for the Crown Court and whilst this alternative remedy exists, it would be wrong for this court to trespass and make an *“Order declaring the application of the MPS’s policy to the Claimant’s criminal investigation and proceedings to be unlawful”* as the Claimant’s pleaded case seeks.

107. Ground Four is dismissed.

Conclusion

108. The claim for judicial review is therefore dismissed.