**MEMORANDUM OF UNDERSTANDING**

**IN RELATION TO DIGITAL EVIDENCE SHARING BETWEEN**

**THE CROWN PROSECUTION SERVICE**

**AND**

**THE NATIONAL POLICE CHIEFS’ COUNCIL (NPCC)**

**ON BEHALF OF EACH OF THE POLICE FORCES**

**LISTED IN ANNEX 4**

This document is classified as OFFICIAL and therefore, Not Protectively Marked, under the Government Protective Marking Scheme and any referrals for advice and rationale in relation to Freedom of Information Act disclosure should be made to the NPCC Central Referral Unit at npcc.foi.request@npfdu.police.uk

**Document Information**

**Protective marking:** OFFICIAL, NOT PROTECTIVELY MARKED

**Force/Organisation:** Digital Case File Team, Police Digital Service

**National Policing Coordination Committee Area:** NPCC Courts Portfolio

**Author:** Neil Edgar

**Contact details:** neil.edgar@pds.police.uk

**Version:** 1.1

**Original Approval Date**: 21/02/2024

**Last Review:** 05/12/24

**Reviewed by:** Staff Officer to ACC Gilmer, NPCC Courts Portfolio Lead

**Next Review date:** 01/12/2026

Any queries relating to this document should be directed to either the author detailed above or the NPCC Business Support Office on business.support@npcc.police.uk

© 2015 – NPCC

**Contents**

[1. PURPOSE AND SCOPE OF THE MEMORANDUM OF UNDERSTANDING 3](#_Toc185589604)

[2. STATEMENT OF OBJECTIVES AND BENEFITS 3](#_Toc185589605)

[3. COMMENCEMENT, DURATION, INTERPRETATION AND AMENDMENT OF THE MEMORANDUM OF UNDERSTANDING 3](#_Toc185589606)

[4. NATIONALLY AGREED STANDARDS 4](#_Toc185589607)

[5. DATA PROTECTION 5](#_Toc185589608)

[6. GATHERING AND RETENTION OF MME 7](#_Toc185589609)

[7. SUPPLY OF MME TO CPS 7](#_Toc185589610)

[8. MME RELIED ON AS PROSECUTION EVIDENCE 8](#_Toc185589611)

[9. MME THAT IS UNUSED MATERIAL 9](#_Toc185589612)

[10. REVIEW OF MME BY CPS 9](#_Toc185589613)

[11. SHARING THE MME WITH THE CJS 10](#_Toc185589614)

[12. Annex 1: Data Controller Responsibilities 11](#_Toc185589615)

[13. Annex 2: MME Blueprint 12](#_Toc185589616)

[14. Annex 3: Photographic Principles\* 15](#_Toc185589617)

[15. Annex 4: NPCC forces of England and Wales 20](#_Toc185589618)

# PURPOSE AND SCOPE OF THE MEMORANDUM OF UNDERSTANDING

* 1. The purpose of this Memorandum of Understanding(**“MOU”**) is to detail the arrangements in place to enable the efficient sharing of multimedia evidence (**“MME”**) by the Relevant Police Force to the CPS via the relevant Digital Evidence Management System Link (**“DEMS”**).
	2. This MOU supports and underpins the existing arrangements in place between the CPS and the Relevant Police Force for the provision of evidential and disclosable unused material and sets out the expected level of service to be provided by both the CPS and Relevant Police Force in relation to the sharing of MME via DEMS.
	3. The MOU is intended to cover all forms of MME that may be shared via DEMS including, but is not limited to, Body Worn Video (BWV), 999 calls, Achieving Best Evidence Video Recorded Interviews, CCTV, still image photobooks and other third-party video material, such as dashcam footage. This MOU is supplementary to any relevant formal guidance or framework relating to MME that has been issued by the UK government, the College of Policing, or the National Police Chiefs’ Council (or similar) (for example, the National Police Chiefs’ Council October 2022) and does not replace any such guidance. To the extent that there is any conflict between this MOU and any such guidance or framework, that guidance or framework will take precedence.
	4. This MOU should be read in conjunction with Annex 1 (Data Controller flow chart), Annex 2 (MME Blueprint) and Annex 3 (Photographic Principles).

# STATEMENT OF OBJECTIVES AND BENEFITS

* 1. The Relevant Police Force and the CPS agree to work in partnership to facilitate the supply of MME from the Relevant Police Force to the CPS, support the use of MME by the CPS and fully recognise the positive impact the Relevant Police Force can have in gathering evidence and supporting the criminal justice system (**“CJS”**). The rapid development of technology provides a significant number of opportunities and benefits to the CJS. The Relevant Police Force and the CPS are both committed to the development of digital working and agree that the provision of DEMS links provides such an opportunity.

# COMMENCEMENT, DURATION, INTERPRETATION AND AMENDMENT OF THE MEMORANDUM OF UNDERSTANDING

* 1. The MOU will take effect from the date of signature below.
	2. It is agreed that this data sharing arrangement to supply MME to the CPS via DEMS link, in accordance with the provisions of this MOU shall be maintained from the date the MOU takes effect. This MOU shall be reviewed at a national level regularly (as a minimum, biennially) to ensure it remains appropriate. Any updated versions will be shared to the parties.
	3. Where either the Relevant Police Force or the CPS wishes to withdraw from the MOU (either partially or wholly), not less than two months prior to the intended date of withdrawal, the withdrawing party is required to give to the other party written notice of its intention to withdraw either partially or wholly from the MOU, including in such notice:
		1. the intended date of withdrawal;
		2. details of the standard or service to be withdrawn;
		3. the reasons for withdrawal; and
		4. a plan for any contingencies that need to be implemented, in order to facilitate the withdrawal.

The parties will discuss in good faith any appropriate and required actions relating to the withdrawal.

* 1. In exceptional circumstances (such as a major security breach), either party may have to take emergency action to suspend normal business activity while checks are made to understand the reasons for the breach, assess severity and actions to take to remedy. The decision for who suspends or agrees business resumption is to be agreed by the Chief Constable (CC) for the Relevant Police Force or Area Business Manager (**ABM**) for the CPS.
	2. Any provision of the MOU may be amended at any time, on the agreement of both the relevant signatories. Amendments must be consistent with any relevant national standards and/or guidance.
	3. This MOU is intended to supplement the already close and cooperative working relationship between the parties. However, from time to time, it is possible that disagreements between the CPS and the Relevant Police Force will arise. Where this occurs, a mutually agreeable resolution should first be sought at an operational level. If a resolution cannot be agreed, the matter should be escalated for discussion between more senior representatives of each party, until such time as an agreement can be reached.

# NATIONALLY AGREED STANDARDS

* 1. The standards for the handling MME via DEMS links will be consistent with relevant national standards, legislative requirements, and policies, and have regard in particular to the guidance set out in the following documents and commitments including, but not limited to:

		1. the Criminal Procedure and Investigations Act 1996 and relevant Codes of Practice;
		2. the National Police Chiefs’ Council (NPCC) Guidance on Body Worn Video 2022;
		3. the guidance to police officers[[1]](#footnote-1) and Crown Prosecutors issued by the Director of Public Prosecutions (**“Director’s Guidance on Charging”**) under section 37a of the Police and Criminal Evidence Act 1984, which has established the requirement for certain categories of charging decision to be made by Crown Prosecutors including the National File Standard;
		4. the National Policing Community Security Policy;
		5. the Code for Crown Prosecutors;
		6. the CPS Casework Quality Standards;
		7. the NPCC National Digital and Physical Evidence Retention Guidance; and
		8. the Attorney General’s Guidelines on Disclosure (**“AGG”**).

# DATA PROTECTION

* 1. In this MOU, the following definitions shall apply:
		1. **“Controller”, “Data Subject”, “Processor”, “processed”, “personal data”, “Personal Data Breach”** have the meanings given to them in the Data Protection Legislation.
		2. **“Data Protection Legislation”** means all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (“DPA 2018”); the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and the guidance and codes of practice issued by the UK’s Information Commissioner or other relevant authority, and which are applicable to a party.
		3. **“UK GDPR”** has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.
	2. It is anticipated that the majority processing of the MME shared by the Relevant Police Force to the CPS via DEMS links will be undertaken for law enforcement purposes by competent authorities and that, consequently, Part 3 of the DPA 2018 will apply.
	3. In relation to any personal data contained within the MME processed under this MOU, the parties acknowledge and agree that:

		1. The Relevant Police Force will be the Controller for all personal data held on a secure police system and the CPS will become a Controller for any personal data that is shared with it via DEMS links by the Relevant Police Force at the point the media is streamed on a CPS device, downloaded or the received DEMS link shared by the CPS. (See Annex 1 for a flow diagram).
		2. Each party shall comply with the Data Protection Legislation in connection with this MOU and neither party shall, by its acts or omissions, cause the other party to breach its respective obligations under the Data Protection Legislation.
		3. The lawful basis for processing the personal data shared via DEMS will be as follows:
			1. the processing is necessary for the performance of a task carried out for a law enforcement purpose by a competent authority (DPA 2018 s35(2)(b)); and
			2. where the processing for any of the law enforcement purposes is sensitive processing, either:
				1. at the time when the processing is carried out, the controller has an appropriate policy document in place (DPA 2018 s35(4)(b)); or
				2. the processing is strictly necessary for the law enforcement purpose, the processing meets at least one of the conditions in Schedule 8 of the DPA 2018 and at the time when the processing is carried out, the controller has an appropriate policy document in place (DPA 2018 s35(5)).
		4. To the extent required by relevant Data Protection Legislation, each party shall ensure that adequate fair processing notices are available for relevant Data Subjects and are sufficient in scope to enable each party to process the personal data as required, in order to obtain the benefit of its rights and to fulfil its obligations under this MOU in accordance with the Data Protection Legislation.
		5. The Relevant Police Force will ensure that an appropriate police officer (the “Officer”) has viewed the MME before its submission via DEMS link to the CPS to confirm it is relevant, is appropriately clipped and/or redacted where necessary and is retained in compliance with the CPIA Code of Practice and the Attorney General’s Guidelines on Disclosure 2022 (as applicable).
		6. The CPS will be responsible for ensuring that any personal data it receives from the Relevant Police Force via DEMS link, is processed in accordance with Data Protection Legislation, any relevant guidance and the DEMS Data Sharing Code at Annex 2. This includes, but is not limited to, ensuring that: (i) the CPS only shares with a third party the information it receives from the Relevant Police Force where strictly necessary for the purpose that it was provided to the CPS or in compliance with the CPS’ statutory requirements and (ii) there is no disclosure of any information shared via DEMS link to an incorrect email address or unauthorised third party.
		7. The Police remain as the Data Controller for all data while it remains on a secure police system, while the CPS becomes the Data Controller for the received links where the link or media is downloaded or shared by the CPS. Where data is streamed from a secure police system to a CPS device, the police are the controller of the stored data and CPS are the controller for the streamed information on their device.
		8. The CPS is responsible for ensuring that the viewing of the media, whether streamed or viewed from a downloaded copy, is done in an appropriate environment where the media cannot be seen or heard by unauthorised third parties.
		9. Defence representatives or His Majesty’s Court and Tribunal Service (HMCTS) become Data Controllers following receipt of the multimedia. CPS have a statutory responsibility to serve evidence on Defence representatives who are then bound by Professional Standards to manage shared data and then become the Data Controllers if downloading or onward sharing any data. This MOU does not cover the handling of data by HMCTS or the defence.
		10. This process is illustrated in Annex1 – Data Controller Responsibilities.
		11. A Criminal Justice Secure email (CJSM) address is required to access any MME provided to the CPS by the Relevant Police Force via DEMS link and it is a CPS responsibility to ensure MME is issued only to such addresses where it is providing access to the MME to its personnel or any other third party.
		12. The CPS shall notify the Relevant Police Force in writing via the Data Protection without undue delay and, in any event, within [twenty-four (24) hours] of it becoming aware of any actual or suspected Personal Data Breach, in relation to the MME still stored on a police DEMS system and shall, within such timescale to be agreed by the parties (acting reasonably and in good faith):

			1. implement any measures necessary to restore the security of any compromised personal data; and
			2. where the Relevant Police Force is the controller of the data, and to the extent required, CPS will provide support to make any required notifications to the Information Commissioner’s Office and/or other equivalent relevant regulator and affected data subjects.
	4. Neither party shall do anything which shall damage the reputation of the other party or that party’s relationship with the Data Subjects.

# GATHERING AND RETENTION OF MME

* 1. Data will be gathered, processed retained, reviewed and disposed of in line with relevant guidance. The retention categories are in line with the current NPCC’s National Guidance on the minimum standards for the Retention and Disposal of Police Records.
	2. Digital Media must be available at every stage of the judicial process and media clips must remain playable and viewable whilst the case is in progress.
	3. The CPS will not retain any MME shared with it by the Relevant Police Force via DEMS links beyond case finalisation and any appeal deadlines in line with its own records management policy.

# SUPPLY OF MME TO CPS

* 1. MME will only be supplied to CPS via DEMS where:

		1. it is to form part of the prosecution case against an accused individual and is required as an exhibit in accordance with the Director’s Guidance on Charging; and
		2. existing processes and guidance require the provision of the MME to the CPS in dealing with unused material in accordance with the responsibilities under common law and those contained in the Criminal Procedures and Investigations Act (CPIA) 1996;
		3. Some material in investigations is now classed as rebuttable presumption material, i.e. material that is presumed to meet the test for disclosure and thus always must be recorded, retained and provided where necessary. A list of this type of material is contained in Paragraph 87 of the AGG.
	2. When requesting a pre-charge decision (“PCD”), the Police will ensure that the existence of any MME exhibits are clearly identified on the MG3[[2]](#footnote-2)  or police pre-charge submission screens (One Way or Two Way interface (TWIF) message LM01/CM01 (Report to Crown Prosecutor for Charging Decision – Review instructions)); at post-charge initial file submission stage, its existence must be recorded on the MG5 (Police Report Case Summary) document, in addition to whether or not it is considered to be relevant evidence.
	3. Any MME provided by the Relevant Police Force to the CPS via the DEMS must be checked prior to submission to the CPS to ensure it is in a playable and viewable format and complies with the National Naming Standards.

# MME RELIED ON AS PROSECUTION EVIDENCE

* 1. MME supplied to the CPS will be provided in a format enabling immediate access to the relevant part of the footage. A secure link with the correct access rights for all CJS parties, will be supplied to the CPS with the pre-charge submission and/or the initial digital case file. Evidential secure links to exhibits must be provided to the CPS on the MG0 or within an LM06 message.
	2. All MME submissions from the Relevant Police Force must be completed digitally via the Police to CPS/DEMS interface.
	3. The Officer must categorise each piece of relevant MME as ‘evidential’ in the DEMS system, to ensure that it is retained for longer than 30 days. To ensure the MME is accessible by all relevant parties, the Officer must ensure that each piece of MME provided is appropriate and capable of being shared with the CPS, HMCTS, and relevant defence counsel and/or external advocates. MME sharing across the CJS is the CPS’ responsibility in line with disclosure legislation and service responsibilities.
	4. Individual secure links will be provided by the Relevant Police Force to the CPS for each piece of MME on separate MG0 documents or LM06 messages.
	5. The Relevant Police Force will only provide the CPS with relevant material. The material should be clipped to the evidential selection before it is sent to the CPS. Ordinarily, the clipped footage should be no longer than 10 minutes. However, if the Relevant Police Force considers there is justification for longer clipped footage, reasoning must be provided in the relevant section of the MG0.[[3]](#footnote-3)
	6. Media should be clipped and stitched together where there are multiple smaller selections of evidential material contained, within a larger selection of recorded footage arising from the same source and event.
	7. All MME should be redacted in line with the Joint National Redaction Principles. If the officer cannot clip or redact the MME for submission for a pre-charge decision, they must provide an MG11 describing the key points of the MME, as per Annex 7 of The Director’s Guidance on Charging- sixth edition (DG6) – Audio-visual evidence.
	8. The secure link will be provided in accordance with the National File Standard requirements.

# MME THAT IS UNUSED MATERIAL

* 1. Unused material is material that may be relevant to the investigation that has been retained, but does not form part of the case for the prosecution against the accused (“unused material”).
	2. Where MME is considered to contain sensitive material (as defined by the Disclosure Manual), it should be handled in accordance with the guidance in the Disclosure Manual. It should be listed and described on the MG6C[[4]](#footnote-4) (Police Schedule of Non-Sensitive Unused material) or Streamlined Disclosure Certificate (SDC). The description must be sufficient to allow the prosecutor to make an informed decision on whether it could satisfy the disclosure test.
	3. Where MME is considered to contain sensitive material (as defined by the Disclosure Manual), it should be handled in accordance with the guidance in the Disclosure Manual. It should be listed and described on the MG6D[[5]](#footnote-5) schedule (Police Schedule of Sensitive Material).
	4. Where MME is considered to require disclosure because it may undermine the prosecution case or assist the defence, an operative secure link will be included with the item description on the Unused Material MG0 document and the relevant endorsement made on the MG6E.[[6]](#footnote-6)
	5. Where MME is considered to contain material that falls within the rebuttable presumption categories it should be shared with the CPS. A DEMS link will be included with the item description on the Unused Material MG0 document and the relevant endorsement made on the MG6E / SDC.
	6. Where Unused Material MME is requested by the CPS for review, the Relevant Police Force will submit the footage on the Unused Material MME document or within the LM07 message.

# REVIEW OF MME BY CPS

* 1. The CPS will review all MME in accordance with the responsibilities detailed in the Code for Crown Prosecutors and the CPS Casework Quality Standards.
	2. The CPS will ensure that all staff have access to approved DEMS.

# SHARING THE MME WITH THE CJS

* 1. The Relevant Police Force will ensure that DEMS is effectively enabled to share relevant MME with the defence counsel and other third parties where appropriate.
	2. Only users with secure email accounts such as cjsm.net and ejudiciary.net email domains, can register for the DEMS platforms.
	3. The Relevant Police Force will ensure that the MME supplied is appropriately clipped and redacted where necessary before it is made available to share, having regard to any relevant guidance.
	4. The CPS will undertake to share MME with the relevant third parties (including defence counsel, external advocates, HMCTS and CPS prosecution agents) via the provision of a secure link where a secure email address is supplied or by uploading the MG0 to the Digital Case System (DCS) or Common Platform uplift (CDES).

**Signatories for both parties**

**SIGNED BY AND APPROVED ON BEHALF OF THE NPCC LISTED IN ANNEX 4**

Signature: ACC Jenny Gilmer (NPCC Courts Portfolio Lead)

**SIGNED BY AND APPROVED ON BEHALF OF THE CPS**

Signature: Matthew Cain (Head of Data Services)

**Original date** signed by both parties: 21/02/2024

**Reviewed and approved** by the parties above on 05/12/2024

# Annex 1: Data Controller Responsibilities



# Annex 2: MME Blueprint

****

**Multimedia Evidence Sharing**

**Design and Development Blueprint**

****

**Design Principles**

The design and development of systems for sharing multimedia evidence (MME) must be based on the following design principles:

1. Digital MME must be capable of being shared with the CPS and directly onward shared with CJS partners following review, i.e. the judiciary, defence and external advocates.
2. Access to the system must be via secure and authenticated means for all users.
3. Relevant metadata must be displayed on the MME within the system.
4. MME must be capable of being both streamed and downloaded.
5. CPS is responsible for disclosure and service of MME across the CJS
6. Digital Media must be available at every stage of the judicial process.
7. When guaranteed access is required (such as when presenting in a court room) a copy of the MME will be downloaded.

**Digital MME must be sharable with CJS partners**

* Any Police MME system must include the functionality for CPS to onward share the links to footage with CJS partners. Police officers[[7]](#footnote-7) must enable the access for all CJS partners at the time of sharing. CPS will then review the MME and serve or disclose by onward sharing the URL in the IDPC or via the Crown Court Digital Case System (DCS).
* A secure and effective method of sharing footage with CJS partners must be available by creating an account-based system authenticated using secure email domains (e.g. CJSM/eJudiciary).
* For service/disclosure purposes each individual URL link should relate to one exhibit. Sharing is via an MG0 template until the capability to send the URL link via the LM06 message into CMS is available (anticipated release in 2023).
* The MG0 documents must be used for both pre- and post-charge submissions over the CJSE into CMS.
* The MG0 document submission must comply with existing naming conventions and logical messaging, with the MG0 being sent via an LM06 message and the Unused MME via an LM07 message.
* The MG5 must not be used to share the URL link due to GAP cases not being reviewed prior to service of IDPC.
* MME must be accessible for the entire duration of a case, including time for the lodging of appeals, and must be retained as per police retention policies.
* Redaction of MME will remain the responsibility of the police if required and redacted MME must be submitted using separate MG0 documents.
* Following receipt of a link CPS are responsible for sharing MME to other CJS parties.

**Access must be via secure and authenticated means**

* Defence practitioners, the judiciary and barristers must access the system through the entry of their secure email address and self-selected password.
* CJSM users must have their secure email address validated at the point of system registration to ensure they are a valid secure email user.
* Password resets must be automatically required after set periods of time to maximise security.
* Auditing functionality must be built into the system but must only be accessible by a limited number of suitably authorised personnel with the right security clearance in a set of specific circumstances.
* URL links must be capable of deactivation if disclosed to unauthorised users.
* CPS access should be through an automated single sign-on process.

**Relevant metadata must be displayed on the MME**

* The exhibit reference and description must be contained within the LM06 message sent to CMS.
* On accessing the URL link, the file size and clip duration must be displayed to indicate the impact it may have on IT infrastructure and the time required for review.
* Where captured, the time and date must be displayed on the MME to aid review and presentation in court.
* Submitted MME must not exceed 10 minutes unless there is a legitimate evidential reason to submit MME longer than this. In these circumstances, an explanation must be included in the MG0 document to prevent automatic rejection. Once the capability to send the URL link via the LM06 message into CMS is available, this information should be submitted using the MG6.

**MME must be capable of being streamed and downloaded**

* Streaming capability is required so MME can be reviewed without the need to download.
* Streaming capability built into the system must be compatible with all mainstream web browsers (e.g. Chrome, Firefox, Edge, Safari).
* Download capability is required to ensure MME can be played in the courtroom without relying on Wi-Fi and to enable defence practitioners to take client instructions from within a custody environment.
* The preferred file formats are .mp4 for video and .mp3 for audio, but as a minimum the MME must be capable of being viewed using VLC Media Player.
* The URL links must be active and directly clickable within an MG0 document sent by the police and in due course in the LM06 message in CMS.
* Additional storage of material must be minimised across CPS and other agencies.

**CPS is responsible for disclosure and service of MME across the CJS**

* Any party that streams media is responsible for doing so in accordance with GDPR requirements.
* Any party downloading media becomes the data controller for that copy of the media and is responsible for its safeguarding and subsequent secure destruction.
* Any party onward sharing media becomes the data controller for that link and is responsible for ensuring that the sharing is secure and to the correct parties.
* Where there is a data breach in relation to inappropriate streaming, downloading or sharing of media the agency that undertook this action is responsible for the breach, liaising to notify the police of the breach and any reporting to the ICO that may be required.

**Digital Media must be available at every stage of the judicial process**

* Media clips must not expire while the case is in progress. It is recommended that clips are not deactivated until the appeal period has concluded.
* Advocates are required to download media for presentation in court as police cannot guarantee 24-hour availability of streaming services and reliance should not be placed on court Wi-Fi.
* Clips may not automatically be retained by police in addition to the core file once a case has concluded due to data storage costs. Where clips are not retained, the metadata of the shared file must be retained.

# See the source imageA picture containing logo  Description automatically generatedAnnex 3: Photographic Principles\*[[8]](#endnote-1)

**Sharing Principles for**

**Photographic & Still Images**

****

**Transfer of Photographs**

* All principles need to be read and accepted before the photobook process can be implemented.
* It is the OICs/disclosure officer responsibility to identify evidential and unused material. Whilst many images will be taken CPS only need to see those which contain evidence relevant to the case.
* Relevant, unused photographs should be recorded on the unused material schedules.
* Officers[[9]](#footnote-8) need to avoid sending the image in multiple views unless appropriate, for example, where a witness has viewed a zoomed in version of a photograph and commented on it.
* Police supervisor must reflect that image selection has been considered with any over/non-selection of images within the photobook being rejected with the officer before submission to the CPS.
* CPS Operational Delivery staff will not play a role in reviewing photographic and rejecting at triage.
* CPS Reviewing lawyers should not delay charging decisions based on an over/non- selection of images unless it poses a detrimental impact on the review. Where substantial over selection has been provided to CPS, feedback should be provided to the Police and a revised photobook requested.
* Where a re-selection is not requested at review stage, is it possible that this may result in increased requests for a revised Jury selection should matters proceed to Crown Court trial.
* It is permissible to send a small number of images via CJS exchange which is CPS’ preferred option. If the image is stored on DEMS and would cause additional work to send via the CJS exchange, then a single image can be sent as a URL via DEMS. Where more than one image needs to be shared via a URL with CPS it must be shared in a photobook.
* Indecent Images of Children - CPS should not receive this material in any format. Images should be described in a schedule and categorised. If these need to be viewed, then arrangements should be made to view them on a police device.
* Sexually Explicit and Graphic Images - This material can be held on CMS and can be sent by police in a photobook URL. However, this material cannot be put onto DCS, as HMCTS have made clear that sexually explicit images (nudity/legal pornographic) and Graphic images should not be uploaded. This is because the DCS has a wider audience than CMS. To be served / disclosure via Secure Email (not via CC DCS). **Prefix file name with ‘Explicit Image’ or** **Prefix file name with ‘Graphic Image’.**

**Evidential Photographic Material**

* The URL for evidential photographic material should be shared via LM06 either within the message or MG0 and with the case material in an MG0 for non-CMS cases. (Holmes/large complex cases).
* Volumes of evidential photographic material should be shared in a DEMs digital photobook.
* Where photos contain personal sensitive data under DPA that are not relevant to the case, these elements should be redacted by the police before sharing.
* Where only selected images are chosen for service on the defence or where the images require relabelling or reorientation, CPS will specify the revised images required and request submission of a new photobook. The whole of the original photobook becomes an item of unused material and the disclosure officer must be notified.
* A number of images from different exhibiting officers can be shared in a single photobook. There must be individual statements produced to exhibit them and the relevant exhibit reference must appear on each image. There is no requirement produce a further statement to exhibit the consolidated photobook. When sending to CMS via the LM06 message leave the exhibit reference field blank. The naming convention should be ‘consolidated photobook’ and description of what it contains. e.g. ‘consolidated photobook – scene of crime’.

**Unused Photographic Material**

* Only unused material that meets the Disclosure Test should be shared in a DEMs Digital Photobook.
* All unused material (does not meet the test for disclosure) should be listed in the unused schedule and not shared.
* The MG6E should identify any photographs the disclosure officer believes either undermines the prosecution case or assists the defence. These photos should be shared in an individual photobook with the disclosure schedule number included in the description.
* If disclosure decisions are different in relation to individual defendants in multi-handed cases, there should be separate photobooks per defendant.
* If additional photographs become disclosable after defence statements are received, an additional photobook should be provided.
* The URL for unused photographic material should be shared via LM07 either within the message or MG0 and with the case material on an MG0 document for non-CMS cases.
* There may be occasions in more serious and complex cases where the reviewing lawyer/prosecution barrister wishes to review unused photographs that the officer thinks does not meet the test for disclosure. If this is the case, it is permissible to share these as a bulk photobook consisting of multiple images from multiple exhibits. The OIC should ensure the prosecutor will be able to cross reference the individual photographs back to the unused schedule. If this is not possible, they will need to be shared as separate photobooks. The prosecutor should provide the justification for the need to view the entirety of the images with the request.

**Jury Presentation**

* Discussion can be held between CPS and Police on a case by case basis to agree on photographic jury bundles to assist court presentation. As CPS do not have case access to force DEMs the only people that can complete this task are the police.
* Where individual photographic exhibits have been served there may be a need to brigade these images into a single photobook for jury presentation. There will be no need to further exhibit this presentational photobook, as the images will have been exhibited already in their own right.
* The CPS will be unable to amend or redact the PDF booklet so there maybe exceptional circumstances where a revised booklet may be required on the day of court. This may be due to legal arguments or exceptional circumstances where the content of the photobook cannot be presented to the jury and a new photobook is required.

**Photobook Content**

* The index of the photobook will show the page number, exhibit reference and exhibit description.
* Officers need to ensure individual photographs are in the correct orientation prior to submission.

**Naming Convention**

* Naming and labelling conventions - The following should be applied in accordance with the National Naming Convention protocol.
* Each still image should be labelled with the description and exhibit reference.
* MG0 (used material) - For consistency, the same MG0 form should be used for NICE Photobooks as for other multimedia. The MG0 should contain the following information:
	+ Type of Media: The term “Image” should be used
	+ Exhibit Reference and Description should follow standard naming convention and be described as ‘Photobook’, e.g. DMD/1 – Photobook of victim injuries
	+ Clip duration should be left blank or “n/a”
	+ Comments: Please note if the exhibit contains any sensitive or distressing material. The comments field should not be used for any other reason.
* MG00 (unused material) – As above but additional fields including Schedule and item number should also be included.
* Naming of the MG00 in integrated case systems - the album should follow format “MG00 Ex DMD1 Photobook of crime scene 280720 [date images captured]
* Clearly an amalgamated photobook will not have a single exhibit so the LM06 message sending field for the X ref should be left blank.
* Naming of the MG00UM in integrated case systems - the album should follow format “MG00UM MG6C Item 6 DMD1 Photobook of crime scene 280720 [date images captured].

# Annex 4: NPCC forces of England and Wales

This Agreement was signed off by the relevant NPCC Lead on behalf of the Chief Constables of NPCC forces of England and Wales (listed below). However, the information sharing will be facilitated by each individual Police Force and the Chief Constable for each Police Force, as Data Controller, has overall responsibility for their compliance with Data Protection legislation.

Avon & Somerset Constabulary

Bedfordshire Police

British Transport Police

Cambridgeshire Constabulary

Cheshire Constabulary

City of London Police

Civil Nuclear Constabulary

Cleveland Police

Cumbria Constabulary

Derbyshire Constabulary

Devon & Cornwall Police

Dorset Police

Durham Constabulary

Dyfed-Powys Police

Essex Police

Gloucestershire Constabulary

Greater Manchester Police

Gwent Police

Hampshire Constabulary

Hertfordshire Constabulary

Humberside Police

Kent Police

Lancashire Constabulary

Leicestershire Constabulary

Lincolnshire Police

Merseyside Police

Metropolitan Police Service

Ministry of Defence Police

Norfolk Constabulary

North Wales Police

North Yorkshire Police

Northamptonshire Police

Northumbria Police

Nottinghamshire Police

South Wales Police

South Yorkshire Police

Staffordshire Police

Suffolk Constabulary

Surrey Police

Sussex Police

Thames Valley Police

Warwickshire Police

West Mercia Police

1. Reference to ‘Officer’ in this document should be considered as any relevant Police staff. [↑](#footnote-ref-1)
2. Following the introduction of the Digital Case File (DCF) system, it is intended that the MG forms will be retired and replaced with new data fields on the DCF system. In this event Officers should adhere to above the principles when completing the new data fields forms introduced by DCF. [↑](#footnote-ref-2)
3. Following the introduction of the DCF System, it is intended that the MG forms will be retired and replaced with new data fields on the DCF system. In this event Officers/staff should adhere to the above principles when completing the new data fields forms. The rational for the inclusion of a longer clip should be included in the confidential information to the prosecutor. [↑](#footnote-ref-3)
4. Following introduction of the DCF System, this will form part of the disclosure process within the system. [↑](#footnote-ref-4)
5. See Footnote reference 4 above on page 12. [↑](#footnote-ref-5)
6. Following the introduction of the DCF System, it is intended that the MG forms will be retired and replaced with new data fields on the DCF system. In this event Officers/staff should adhere to the above principles when completing the new data fields forms. The rational for the inclusion of a longer clip should be included in the confidential information to the prosecutor. [↑](#footnote-ref-6)
7. Reference to ‘Officer(s)’ in this document should be considered as any relevant Police staff. [↑](#footnote-ref-7)
8. \*The principles in this document are for use in volume crime cases only. A separate document will be developed for Major Crime and Complex Crime Unit case. [↑](#endnote-ref-1)
9. Reference to ‘Officer(s)’ in this document should be considered as any relevant Police staff. [↑](#footnote-ref-8)