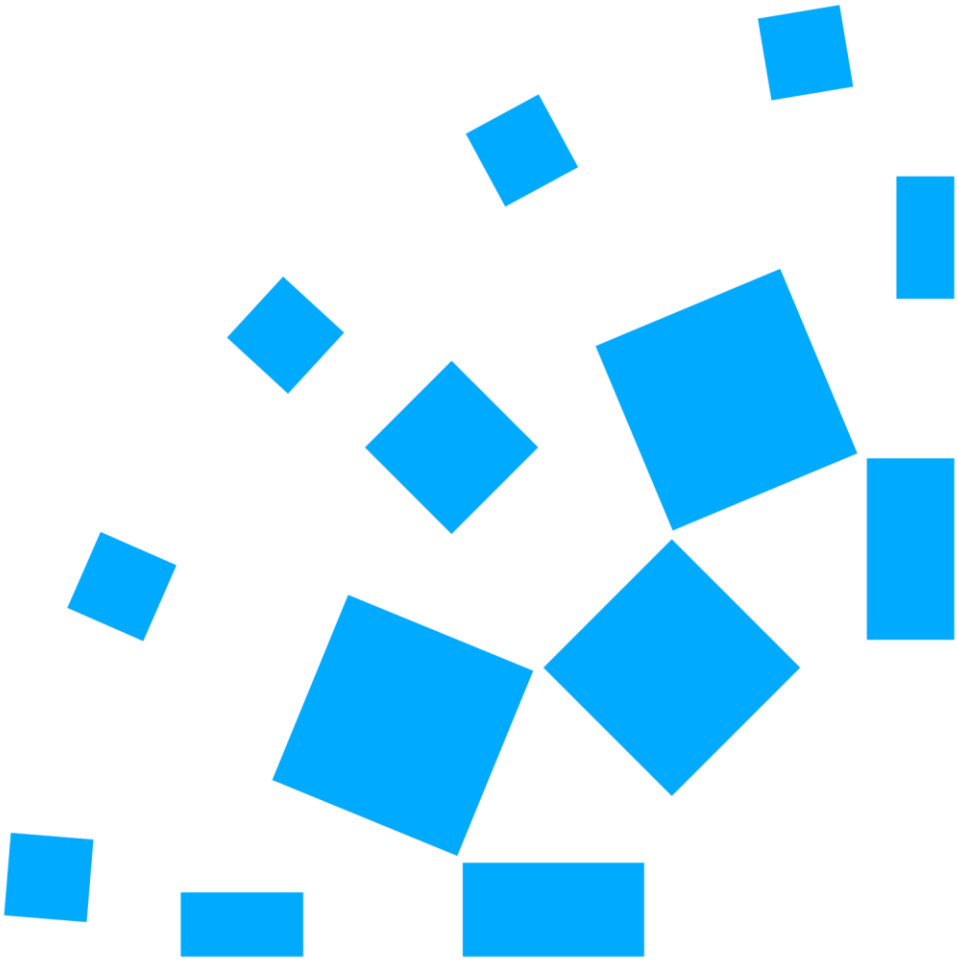
College of Policing

Working together
to share knowledge

This document had been superseded by the latest guidance.

Search the National Police Library Catalogue for the updated version

https://www.college.police.uk/research/library



NATIONAL CCTV WORKING GROUP

OFFICIAL

NPCC Framework for Video Based Evidence

Produced by the NPCC CCTV Working Group, in consultation with the Forensic Science Regulator, DSTL, Surveillance Camera Commissioner's office and national CCTV leads.

Contents

Preface 3
Document summary and purpose 5
NPCC National CCTV Framework 7
Framework Rationale 8
Training levels 10
Activity levels 12
Training and Competency Levels 15
First Responder L0 Awareness Training Definition: 15
Staff / Officer Initial Training Level 1 Definition: 15
Staff / Officer Technical Training Level 2 Definition: 16
Staff / Officer with Forensic Specialist Training Level 3 Definition: 16
Risk matrix 18
Recovery activities by level 35
Level 0: 35
Level 1: 35
Level 2: 35
Level 3: 35
Dependent on valid method 35
Links to relevant documentation: 36

Preface

To Chief Constables, Investigation and Forensic Leads

All Police Forces
8th July 2022

I am writing to advise you of the publication of the NPCC Framework for the use of Video Evidence.

In 2019, I tasked the national CCTV working group to review all existing material that relates to the management and processing of CCTV, ensuring we cover the whole end to end lifecycle of CCTV. Much of this material was out of date and no longer relevant to recent technical advancements and challenges. This has led us to review not just the existing College of Policing (CoP) material but also other training and procedural guidance that is being used across law enforcement. Our aim is to provide updated process and training material to support a more effective and efficient way of managing CCTV evidence across law enforcement. I am pleased to report that this significant work is now reaching its conclusion.

The National team have been working through all existing CCTV guidance documents and training material and have identified changes that are needed to bring them up to date and comply with the Forensic Science Regulator's Statutory Code.

The first of these 'The Digital Image and Multimedia Procedure v3.0', is currently available on GOV.UK. The second, the 'Recovery and Acquisition of Video Evidence v3.0' procedure has been published this month and guides the procedure of securing and preserving this evidence.

In addition to these updates, and to ensure national compliance with the FSR's Code, the team have produced the attached NPCC Framework for the use of Video Evidence that highlights the minimum requirements to UK Policing in order to comply, this framework mitigates the risks identified and highlights the minimum training requirements for officers and staff to handle this evidence in a professional, clear, and transparent way.

This document shapes APP and training and the College of Policing have already started to update and develop the currently available training to meet these requirements this updated training will be available by the end of this year.

It is our intention that these documents will give the FSR the confidence that UK Policing will deliver the training and competence and not require any further mandated accreditation for video evidence outside of forensic laboratories.

The overall implications to policing are minimal, training around these aspects should already be in place within policing and being updated by the CoP so will only require more formal and mandatory delivery and CPD recording to prove competence of those staff involved with this area. This will professionalise a key area of evidence that has to date been overlooked with regards to its importance and benefits, decrease the number of missed opportunities and increase detections.

The Framework document should be shared widely within your forces to those with the remit to handle and process CCTV evidence from recovery to court.

Kind regards,

ACC Jenny Gilmer – NPCC Lead for CCTV

Document summary and purpose

This framework is relevant to police non-specialist front-line staff and forensic units[i] who utilise video evidence, including activities relating to recovery, acquisition, viewing and processing of CCTV.

This document has been created to support the recommendations of the NPCC CCTV Working Group and Specialist Capability Network, and also supersedes the now defunct Annex A and B CCTV Scope for Accreditation document, which was previously circulated by the NPCC as a supplement to the non-statutory Forensic Science Regulator's Code.

The Forensic Science Regulator Act 2021 resulted in the creation of the statutory Forensic Science Regulator and the issuance of a statutory Code of Practice which replaces the previous Codes of Practice and Conduct. The new statutory Code of Practice specifies specific requirements for all those performing the forensic science activities (FSAs) it defines. In the case of video this is FSA–DIG 300– Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS) and the FSA – DIG 301 – Specialist video multimedia, recovery, processing, and analysis.

Those performing FSAs are required to comply with the statutory Code[1], and any associated FSA specific requirements (i.e., section 109 of the Code, Video processing and analysis). When required by the Code, those performing certain FSAs require to be accredited to BS EN ISO/IEC 17025:2017 for that activity (such as the extraction, preservation, production, and analysis of video material), or if acting in accordance with this framework perform the more limited specified range of activities in the FSA "DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS)" without accreditation provided the competence and governance requirements are met.

This Framework document identifies, but not exhaustively, the risks identified with the use of a non-accredited / non-competent approach for Recovery, Acquisition, Viewing, Production for court, and evidential storage/transfer. Risks can be mitigated to varying degrees by suitable standard operating procedures, competency, training, and awareness.

[1] https://www.gov.uk/government/publications/statutory-code-of-practice-for-forensic-science-activities

This framework can equally be applied to audio data as per the Home Office DSTL NPCC Digital Imaging and Media Procedure V3.0. [2]

It is critical to understand digital video and audio recordings must be treated with the same care as other forms of digital evidence (e.g., phones/computers) from the outset of an investigation.

This framework including the risks highlighted in the Risk Matrix must also be considered for specialist expert activity such as facial image comparison[3] and photogrammetry and should be considered when using an external or internal accredited specialist forensic providers.

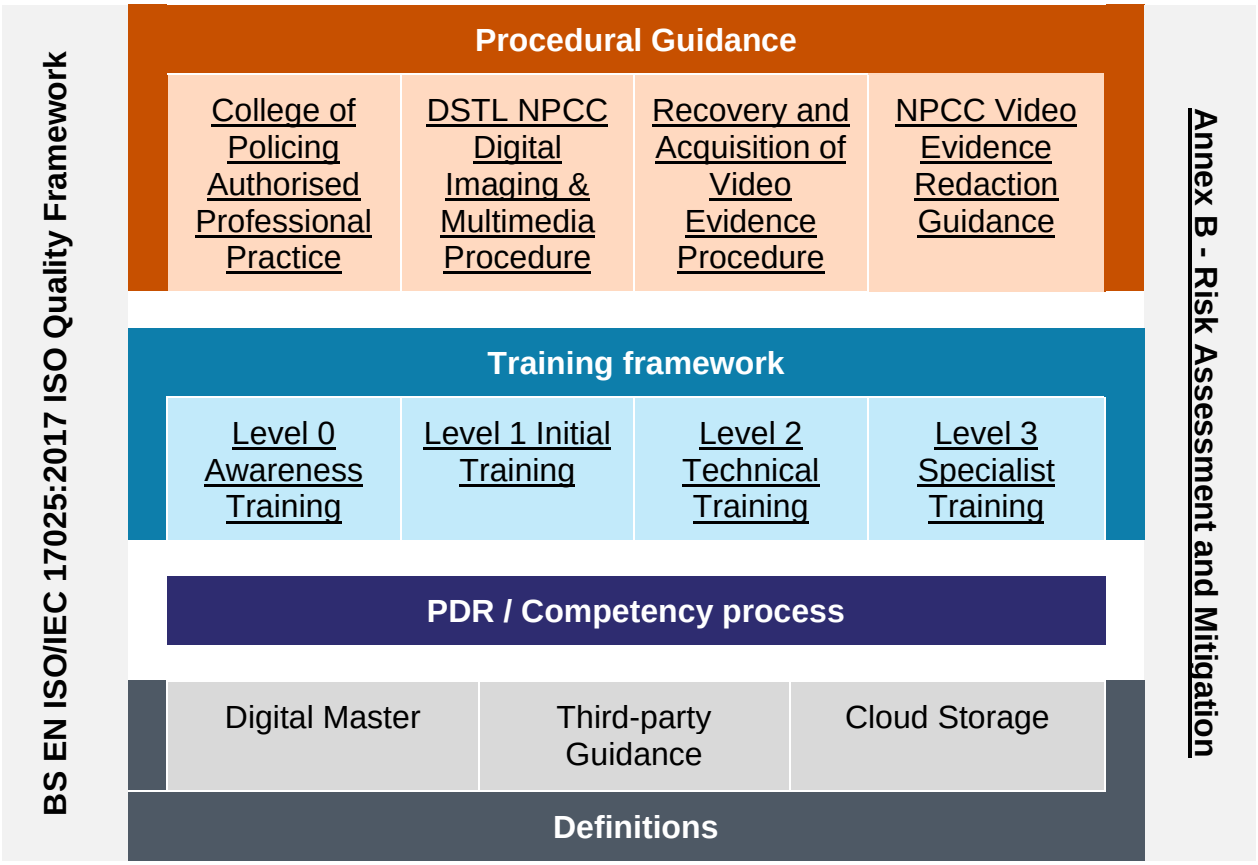
Links within the Framework will take you to the appropriate documentation, whether it be legislation, guidance, or training, to provide a complete and comprehensive approach to how CCTV should be managed within policing.

[2] https://www.gov.uk/government/publications/digital-investigations-digital-imaging-and-multimedia-procedure
[3] FSR Regulatory Notice 01/2019 Image Enhancement and Image Comparison: Provision of Opinion

NPCC National CCTV Framework

NPCC National CCTV Framework

Underlined sections below are links to external sources or areas in this document.



The Forensic Science Regulator considers CCTV to be a forensic science activity discipline, and under the Code of Practice is specifically listed alongside Digital Forensics. Therefore, it is subject to the same obligations to implement quality standards and accreditation as any other area of forensics. However, historically CCTV has not received the resourcing, investment or attention that is currently being directed to other areas of forensic science, in particular digital forensic units, via the recently funded Transforming Forensics programme.

Inadequate resourcing, training, and procedures within police video labs (and in areas of policing outside the video labs) results in missed opportunities and poor-quality video evidence being recovered and submitted to court. Analysis and interpretation methods that have not been validated could be challenged by defence teams. Quality failings in video analysis is an issue that has regularly been referred to the Forensic Science Regulator, from missed opportunities, wrong identifications, and miscarriages of justice.

Framework Rationale

PoFA, GDPR / DPA, CPIA, DSTL Digital Imaging and Multimedia Procedure V3, ACPO Good Practice Guide for Computer-Based Electronic Evidence[4] and DSTL Recovery and Acquisition of Video Evidence Procedure must be considered when carrying out actions with digital CCTV evidence. They outline the process of acquiring and processing CCTV data and additionally enforce the following ACPO principles:

Principle 1:
No action taken by law enforcement agencies, or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2:
In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3:
An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third-party should be able to examine those processes and achieve the same result.

Principle 4:
The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

The above ACPO principles outline the necessity to maintain the continuity and integrity of evidence, and to demonstrate how evidence has been acquired, showing each process,

[4] ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

through which the evidence was obtained. In addition to these requirements, it is also essential to display data objectivity in a court.

Master evidence must be preserved to such an extent that any suitably trained third-party is able to repeat the same process and arrive at the same result as that presented to a court.

The Forensic Science Regulator's Code requires all forensic science activities to be undertaken by trained and competent staff, with specialist departments under a BS EN ISO/IEC 17025:2017 ISO quality framework of accreditation. However, the Regulator has made dispensations for certain front-line activity, provided it is be performed by trained and competent staff using standard operating procedures or simple manufacturer intended methods, such as the owner would use. This document therefore also includes those various processes and procedures that are permitted to be undertaken outside of accreditation. The training referred to in this document represents the work of the NPCC CCTV Training and Ways of Working Strand including awareness, competence, certification, and advanced training for processes, and supports those activities following Force Standard Operating Procedures.

Accreditation is the recognition that an organisation has been formally deemed competent to complete certain activities in a reliable, and accurate manner. Accreditation relates to a wide range of businesses across all sectors and is internationally recognised. Gaining accreditation has several benefits. It is the preferred approach for gaining public confidence in the quality of the work that is completed, in this instance by your forces visual/imaging units ensuring that maximum quality and security is maintained at every stage during the process. Similarly, it offers validated processes which can be repeated and checked.

Although there is some cost in gaining accreditation; the cost relates to the size of your operation and what is being undertaken. There are several steps to achieving accreditation ranging from the very beginning- enquiring if accreditation is required, purchasing the latest standard documents, developing SOPS, Training, Competence assessments, and so forth. A guide can be found on the UKAS website. Once attained it must be maintained to retain the accredited status, this is done via audits from UKAS which review your process, at these audits you can maintain your accreditation, have recommendations, lose accreditation or have it suspended.

Training levels

The following chart show the expected levels of training required to carry out those activities, starting at level 0, first responder officers with Initial Police Learning and Development Programme (IPLDP)/CollegeLearn (formally MLE) training, and escalated by complexity to those roles with the appropriate training levels. Staff should not operate outside of their area of competency in order to comply with The Forensic Science Regulator Act (2021).[5]

<table>
<tr><th>Training Level</th><th colspan="5">ACTIVITY</th></tr>
<tr><td>Level 0
First Responder</td><td colspan="5">CCTV acquisition from third-party/owner operator</td></tr>
<tr><td>Level 1
Initial Training</td><td rowspan="2">For level 1 and level 2:
CCTV acquisition/retrieval at scene or relevant venue by trained Police/staff, using a simple manufacturer’s intended method or escalated to level 2, where further competency/skills are required</td><td colspan="2">Investigative viewing of CCTV</td><td colspan="2">Creation of stills for PACE code D recognition only</td></tr>
<tr><td>Level 2
Technical
Training</td><td colspan="2">Conversion to viewable format using validated processes, where native format is still available</td><td colspan="2">Basic compilation of footage using SAI approved DEMS/DAMS</td></tr>
<tr><td>Level 3
Forensic
Specialist
Training under
ISO-17020/5</td><td>Image analysis</td><td>Specialist CCTV retrieval (lab-based) using non-standard methods</td><td>Image correction and enhancement</td><td>Advanced editing and compiling of footage/data</td><td>Data recovery (from non-working systems metadata analysis)</td></tr>
</table>

[5] https://www.legislation.gov.uk/ukpga/2021/14/contents

Level 0 First Responder	Activity following DII Op Modify[6] digital scene awareness, not in scope of Forensic Science Regulator Code but following CPIA exhibit handling procedures.
Level 1 Initial Training	Activities following FSR Statutory Code undertaken using force approved methods, systems, procedures, and training that follows published national guidance and legislation with level 1 awareness training.
Level 2 Technical Training	Activities following FSR Statutory Code undertaken using force approved methods, systems, procedures, and training that follows published national guidance and level 2 competency certificated training.
Level 3 Forensic Specialist Training under ISO-17020/5	Forensic process carried out under ISO17020/5 accreditation following FSR Statutory Code, using validated methods of processing and analysis with training and competency to advanced levels.

Training Level	College of Policing Provision
Level 0 First Responder	IPLDP training delivered to all officers, along with evidence-handling techniques and DII Op Modify digital scene awareness.
Level 1 Initial Training	College Learn CCTV Retrieval Course, or in house delivered training to front line staff/officers likely to be hands on with CCTV systems/evidence during the course of their role. Recovery of footage from digital CCTV/VSS in situ by methods approved by the SAI that incorporate the CCTV/VSS system manufacturer's intended method: export video or extraction of removable media intended by the manufacturer.
Level 2 Technical Training	Following the mandatory L0-1 training, College of Policing Advanced Skills in CCTV Retrieval/Acquisition Course delivered in-house to specialist technical staff/officers whose core role is acquisition and recovery of CCTV evidence. Where acquisition/retrieval exceeds the skill set for L2 the activity must be escalate to level 3 staff who have received advanced forensic training.

[6] Op Modify is an interactive resource that has been developed by the College of Policing to develop Police understanding of digital opportunities for intelligence and investigation.

Level 3 Forensic Specialist Training under ISO-17020/5	Training for forensic level 3 activities need to be decided by individual forces, to ensure compliance with the requirements of the FSR Statutory Code, ILAC-G19 and ISO17025.

Activity levels

Level 0 - First Responder	
CCTV retrieval from third-party/owner operator	Where CCTV footage is downloaded by system owner or operator, the requesting officers should be cognisant of the Dstl Digital Imaging and Multimedia Procedure and Dstl Recovery and Acquisition of Video Evidence Procedure have received awareness training and must check time/date noting no. of cameras at scene and must check the download ASAP (correct footage present). , The overarching requirement is to be able to show that the recovered footage is true to the original video recording and remains so from the point of recovery; in practice any exported footage should be a bit-for-bit copy of the original wherever possible with a method to show it has not been tampered with. Don't record the CCTV screen using any recording device, if unsure escalate to level 1 staff for guidance who have received competency/training.
Level 1 - Initial Training	
Investigative viewing of CCTV	Viewing of CCTV correctly and with sufficient quality to make a clear judgement of events. The activity performed at this level is viewing with no further analysis. The FSR Statutory Code FSAs contain further detail on the extent of the accreditation element of this requirement for activities such as CCTV replay conducted by competent staff using methods approved by the organisation. Except for provisions in PACE Code D, no exemption from accreditation requirements should be inferred where opinion is required to be given in evidence.

Creation of Stills E.g. ID Sought	Creation of stills/ID sought images using force approved methods (e.g., DEMS, Kiosk based systems) ensuring there is no degradation or distortion of images produced. The nature of the transformations introduced by tools used for exporting video and stills from CCTV shall be assessed so that their impact on the subsequent use of the transformed material can be determined.
CCTV acquisition/retrieval **At scene/venue by trained Police/staff, using manufacturer's intended methods**	Activity crosses two levels of training following on-line basic CCTV recovery and further certificated training by Police officers/staff, following the Dstl Recovery and Acquisition of Video Evidence Procedure and have received firstly basic training to ensure preservation of the native format. L1 only using system designed methods of retrieval (Disc/USB). and checking the download ASAP. **Don't screen record footage!** further escalate in difficult circumstances to level 2 certificated staff who have received core skills training, (cloud download/Network). Where acquisition/retrieval exceeds the skill set for L2 the activity must be escalate to level 3 staff who have received advanced forensic training where further competency/skills are required.
Level 2 -Technical Training	
Conversion to viewable format, using validated systems	Converted formats are for viewing purposes only where no further analysis/processing is required. Carried out using force approved methods (e.g., DEMS/DAMS, specialist CCTV/Imaging systems) ensure the original native master exhibit is preserved for further use if contested.
Basic clipping and compilation of single source footage, using validated DEMS/DAMS	Must be carried out by trained and competent officers/staff authorised to use force SAI approved DEMS/DAMS systems; clipping and compilation of a sequence from a single multimedia source/system, insertion of titles redaction of visual and audible data.
Level 3 - Forensic Specialist Training under ISO-17020/5	

Specialist CCTV acquisition using non-proprietary methods	Following forensically sound methods of downloading of CCTV from systems that have been seized and taken to specialist units. This includes using manufacturers methods as above and also non-standard methods/software such as non-standard networking software. Forensic units providing video analysis shall comply with the Code of Practice and Conduct (The Code), and when required by the Code, be accredited to ISO17025 for any laboratory activity (such as the recovery, preservation, production and analysis of video material).
Advanced editing and compilation of footage	Using validated tools for; creation of any compilations of multimedia and data from multiple sources/systems, synchronisation, annotation, redaction of persons/areas of interest, speed adjustment, scaling and cropping.
Image correction and enhancement	Application of any filters or techniques that aid viewing or identify key areas of the footage that are not easily identifiable from the source material. This includes brightness/contrast, gamma, levels, saturation, de-interlacing, unsharp mask, noise reduction, frame averaging, aspect ratio adjustments.
Image analysis	Including facial/object comparison, height analysis, speed analysis, gait analysis, and timing calculations.
Data recovery/extraction metadata analysis	Recovery of data from discs, USBs, Hard drives using validated systems (from non-working systems e.g., File carving, DVR Examination tools).

Training and Competency Levels

First Responder L0 Awareness Training Definition:

It is critical to understand the difference between levels. This level, level 0, only concerns receipt of evidence from owner/operator using evidence handling as per IPLDP officer training, with no operation of the CCTV system. Awareness training is provided to all new recruits through the College of Policing initial entry routes e.g., College Learn Op Modify, IPLDP, PIP.

First responders are personnel who are the first to identify, secure, preserve, and/or collect CCTV Images and Data at a scene.

- A first responder for volume crime may be an officer tasked with collecting CCTV evidence that has been downloaded by the system owner or their installer or gathering information about the CCTV system to facilitate a Level 1,2 or 3 technical download request. This role may include exhibit handling and taking of CCTV witness statements.
- A first responder for major crime may be an officer allocated trawl duties, to identify CCTV opportunities around a scene or route, collecting CCTV evidence that has been downloaded by the system owner or their installer (including exhibit handling and taking of CCTV witness statements), and gather information about CCTV systems to facilitate a technical download request.

Staff / Officer Initial Training Level 1 Definition:

Training (including internally delivered) specifically for basic CCTV activities must be to nationally recognised learning standards e.g., College of Policing Learn Foundation Skills in CCTV Retrieval or through relevant national training. Retrieval via the operation of working machines, in situ, by manufacturers intended and documented methods is taught at level 1 and level 2. The distinction between the levels of training is that Level 2 training provides an enhanced knowledge of a wider range of equipment. Level 1 training however covers a lower level of image capture and presentation.

Staff / Officer Technical Training Level 2 Definition:

Training specifically for higher CCTV activities must be provided by the College of Policing Advanced Skills in CCTV Retrieval or through relevant national training. These personnel will have a responsibility for the recovery and acquisition of CCTV images and data using force approved methods/SOPs of evidential export or technical data recovery. Strictly following the Home Office DSTL Recovery and Acquisition of Video Evidence Procedure[7].

At level 2 retrieval is operation of working machines, in situ, via manufacturers intended and documented methods. Distinction between levels is training and equipment and allows for networking but not specialist forensic tools. Basic clipping and compilation of single source footage by validated and force approved tools within a DEMS/DAMS system is permitted by trained competent staff, covered by published documentation & SOPs.

The requirement of competency must remain, preventing practitioners from blindly implementing procedures which they do not first understand.

The accreditation exemption is to allow investigating officers to have risk-controlled access to the material they need, it is expected that video laboratories may also hold accreditation to cover the entire spectrum of its offering to investigation officers, not only the level 3 activity.

Staff / Officer with Forensic Specialist Training Level 3 Definition:

Training provided to specialist forensic roles must adhere to the requirements stipulated by the Forensic Science Regulator's statutory code. Training may be externally provided or through relevant in-house training. Those carrying out level 3 activities must regularly demonstrate their competency through in house assessment/CPD. Anything not covered in level 1-2 above, and any processes carried

[7] https://www.gov.uk/government/publications/recovery-and-acquisition-of-video-evidence

out in a lab environment, must be covered by BS EN ISO/IEC 17025:2017 accreditation.

These personnel have a responsibility for the acquisition of CCTV Images and Data via methods of evidential export or technical data extraction using advanced techniques and complex software tools. They also prepare video and image evidence for examination, analysis, and presentation. They identify file formats, establish best methods of preserving image quality and integrity while converting and capturing the imagery in the most appropriate output format in line with the customer requirement.

Personnel who carry out analysis, enhancement, data recovery, advanced compiling and expert or opinion-based reports also must adhere to the Level 3 training and competency requirements.

Risk matrix

The below risks have been identified internationally by digital evidence and media practitioners and must be considered when providing services and processes outlined, being cognisant of the training levels required for each process. Each risk is not exhaustive to each section and may be applicable to other sections.

It is advisable to apply the following guiding principles[8] or similar for export and file preservation to mitigate these risks:

1) **Do no harm** – with export, preserving the native video quality captured by the CCTV system thus avoiding transcoding and recompressing.

2) **Promote key metadata** – starting with date and time (with future provisions for location and camera metadata)

3) **Leverage existing standards** to the extent feasible (when no prudent or feasible alternative exists and all possible efforts to comply with regulations and minimize potential harm or adverse impacts have been undertaken).

4) **Use a flexible container** – selecting a format that supports general playability and multiple data streams ideally at the same level of quality as on-board the original system.

5) **Minimize cost** – aligning the standards solution as closely as possible to Industry's common export features and codecs, leading to increased acceptance and adoption, while minimizing cost to the end user.

Recovery/acquisition: **Follow the DSTL NPCC Retrieval of CCTV guide for use in criminal investigations**				
Ref	**Cause**	**Event/effect**	**Impact**	**Mitigation/Action**
1	Failure to complete or correctly record system date and time against real time.	Incorrect data recovered / required data lost.	Loss of evidence and wasted investigative time.	Follow first responder awareness training[9].

[8] NISTIR 8161r1 Recommendation: CCTV Digital Video Export Profile – Level 0 (Revision 1)
[9] CollegeLearn Operation Modify: Improving Digital Thinking

2	Retrieval itself includes file conversion.	Potential drop in resolution, compression, lost frames, frame rate effects and loss of metadata.	Value of evidence reduced or lost. Effects on PACE code D identifications due to loss of definition. Loss of time and date information.	Ensure awareness training, process and policy is in place where identification is required.
3	'Acquisition' by videoing the display monitor with a smartphone or body worn camera at premises.[ii]	Extreme form of file conversion and should be avoided even if this is used when all other options have been exhausted. Contamination with environmental audio and reflection of officers.	Distortion and degradation of quality. Lost evidential opportunities, and reputational risks also occur. Inability to carry out further analysis/identification.	Ensure policy is in place to negate this practice. Ensure acquisition is carried out correctly by L1 staff. Follow first responder awareness training.
4	Removal of internal hard drive from Digital CCTV system results in damage to HDD / System.	Damage to internal data storage or system or automatic re-formatting when replaced.	Loss of evidence, although reputational risks also occur. Also, loss of owner's data and potential for claims against police for damage.	Ensure, process and policy are in place. To ensure only authorised L3 staff carry this out.
5	Recovery of data from removed / internal storage drives requires specialist expertise and systems.[10]	There may not be a way of retrieving imagery from the HDD after removal, use of tools designed to do this may not display and extract all imagery or may misinterpret the data.	Loss or destruction of evidence, and reputational risks also occur. Also potential for claims against police for loss or damage.	Ensure processes and policy are in place and ensure recovery is only carried out by L3 staff.

[10] Section 109 of the Code, Video processing and analysis

		If no extraction tool can be found, then the imagery will need to be extracted using complex data recovery methods that are extremely time consuming		
6	Replay software (if available) is not downloaded from system alongside the evidence.	Effect is that evidence may not be viewable. If incorrect software is used, whilst the images can be replayed, it displays images or metadata (time/date) poorly or incorrectly.	Extra time is required later to find the appropriate software, or it is believed it is not viewable and evidence lost.	Ensure policy is in place. To ensure recovery is correct. Operate and purchase up to date equipment with as many relevant proprietary players.as possible
7	Inexperienced user could accidentally alter settings and configuration of the CCTV system itself whilst carrying out the retrieval.	Owner is left with a malfunctioning or incorrectly setup CCTV system.	Loss of confidence in the police, reduction in cooperation. Potential loss of future evidence if system left not recording correctly. ICO fines and reputational damage.	Ensure process and policy is in place to ensure only trained staff carry this out. Legal departments should be aware of potential liability.
8	Insufficient understanding of the system settings.	Incorrect period retrieved or incorrect camera views.	Loss of evidence. Misleading information that can confuse investigation process.	Follow first responder awareness training

9	Insufficient recording of the system settings, the system make and model number and position of cameras, overwrite times, time lapse or motion detect settings, and remote connectivity for viewing via smartphone etc.	Ambiguity of time and critical system settings e.g.: motion detection remote connectivity.	If noticed - Investigative time is wasted verifying correct time or issue of relevance is raised at court. If not noticed - Loss of evidence, wrong period retrieved/viewed. Effect on future analysis. EG frame rates and camera settings are critical for further speed analysis.	Ensure recovery is carried out correctly by trained staff. Follow first responder awareness training.
10	Recording is not labelled correctly.	Continuity issues, unclear where it refers or simply gets misfiled or lost.	Loss of evidence. Potential for ICO fines and reputational damage.	Ensure basic exhibit handling training is up to standard. Follow first responder awareness training.
11	Specialist recovery is requested or mandated and unavailable.	Data is not collected before it is overwritten by the system.	Loss of evidence and reduced public confidence in the police.	Engage with L2/3 staff in advance of any issues arising.
12	Deletion of the data during recovery process (e.g., while accessing an unfamiliar system).	Data lost.	Loss of evidence, although reputational risks also occur. Additionally, loss of owner's data and potential for claims against police for damage.	Follow first responder awareness training. Ensure only trained staff carry this out.
13	Deletion of the data once the copying is reported to be complete (e.g.,	Data lost.	Loss of evidence, although reputational risks also occur. Also, loss of owner's data and potential for	Follow first responder awareness training. Ensure only trained staff carry this out.

	responding to a prompt).		claims against police for damage.	
14	Incomplete data recovery. (e.g., missing relevant metadata/cameras)	Data lost.	Loss of evidence, although reputational risks and defence criticism also occur.	Follow first responder awareness training. Ensure only trained staff carry this out.
15	Physical loss of the recovery media.	Data lost.	Loss of evidence, although reputational risks and Data Protection/GDPR and MOPI issues also occur. Potential large fines from ICO and costs associated. Internal disciplinary procedures and changes to procedures.	Ensure basic exhibit handling training is up to standard. And data handling procedures are robust.
16	Seizure of system.	Electrical safety and damage to system if incorrect power supply used. Leaves premise un-protected, removes owners' access to their data.	Licencing issues where premise requires CCTV reputational risks also occur. Also, loss of owner's data and potential for claims against police for damage. GDPR DPA18 issues.	Ensure systems are in place to provide guidance for system removal and to ensure copying and return is completed as efficiently as possible along with loan units where required. Ensure only trained staff carry this out.
17	System has 'data retention' period active, hiding / deleting any data retained after this period.	Data is not collected.	Loss of evidence.	Follow first responder awareness training.

18	Certain cameras are 'covert' and hidden during playback from the system.	Data is not collected, hidden cameras missed.	Loss of evidence.	Ensure awareness and training is in place. Liaise with L2/3 trained staff.
19	Incorrect use/control of removable media.	Data corrupted or systems corrupted. Failure to sanitise removable media prior to use and following transfer to secure medium/storage results in data being uncontrolled and or contaminated.	Loss of evidence, although reputational risks and Data Protection/GDPR and MOPI issues also occur. Potential large fines from ICO and costs associated with subsequent internal disciplinary procedures, organisational learning and changes to procedures.	Ensure own Force policy, reporting process, awareness and training is in place.
20	Owner of system carries out their own download and provides it to the police physically or via direct upload.	Any number of the above risks can occur, and the police will not know which and to what degree. This will depend on the owner's competence in providing the correct native format.	Inability to be clear and prescriptive about what has been recovered.	If owner cannot provide the evidence correctly in its native format. Trained police employees to advise wherever possible or carry out downloads.
21	Recovered footage not tested at scene before the officer carrying out the recovery leaves the premises.	Incorrect footage recovered or footage does not play / is corrupted.	Loss of evidence.	L3 Officers / staff carrying out downloads to be equipped with suitable equipment to check their work before leaving the premises.

22	Data stored in online / cloud systems is not accessible by OICs.	Footage not available due to force IT restrictions or accessible in a timely manner.	Loss of evidence or wrong format downloaded / provided.	Trained police employees to carry out downloads wherever possible.

Surveillance Camera Commissioners Statutory Code of Practice states:

4.11.2 - It is important that there are effective safeguards in place to ensure the forensic integrity of recorded images and information and its usefulness for the purpose for which it is intended to be used. Recorded material should be stored in a way that maintains the integrity of the image and information, with particular importance attached to ensuring that metadata (e.g., time, date and location) is recorded reliably, and compression of data does not reduce its quality. This is to ensure that the rights of individuals recorded by a surveillance camera system are protected and that the material can be used as evidence in court. To do this the medium on which the images and information are stored will be important, and access must be restricted. A record should be kept as an audit trail of how images and information are handled if they are likely to be used as exhibits for the purpose of criminal proceedings in court. Once there is no longer a clearly justifiable reason to retain the recorded images and information, they should be deleted.

Viewing/Playback: - Following the Home Office, DSTL, NPCC, APP, CPIA guidance				
Ref	**Cause**	**Event/effect**	**Impact**	**Mitigation**
23	Force decides not to have an in-house specialist service.	There is no specialist review.	Excess submissions or specialist role creeps into non-specialist viewing in an unmanaged way resulting in inconsistency and different working practices across teams. Limited ability to review evidence supplied by witness	Clear guidance and working practices. Potential inter- force collaborations

			that will affect public confidence in the police/CJS.	
24	Late request for specialist service.	Insufficient time to perform specialist processing/technical requests.	Evidence not presented in court. Impact on public confidence.	Ensure those submitting requests understand realistic time frames.
25	Working Copy not made.	Over processing of images using destructive methods using the only available copy.	Enhancement/clarification of image is challenged in court. Original images must be used, failure to do so results in loss of evidence or challenge in court.	Clear guidance and working practices.
26	Creation of working hard copies not recorded.	Continuity issues. Non-compliance with ICO, DPA/2018 and GDPR information security.	Loss of evidence, although reputational risks and Data Protection/GDPR and MOPI issues also occur. Potential large fines from ICO and costs associated with subsequent internal disciplinary procedures.	Clear guidance and working practices.
27	Master copy not defined.	Continuity issues.	May hamper further analysis resulting in loss of evidence or challenge in court.	Clear guidance and working practices.

28	No available Replay Software.	Viewing not possible.	Time lost by investigators or evidence lost. Incorrect software could lead to loss of on-screen timecode or other metadata. Whole cameras not being replayed, horizontal aspect ratio being halved due to de-interlacing, or edges of camera view being cropped.	Forces to invest in up-to-date equipment and processes that ensure native data and replay software is secured at point of seizure.
29	Detail is lost or not visible in the Replay Software selected or due to file conversion.	Action or events missed or lost. Replay of evidence is inhibited or unreliable due to file conversion.	Value of evidence reduced or lost, Effects on PACE code D identifications due to loss of definition and competency challenged in court.	Ensure awareness and training is in place.
30	Replay Software does not handle multiplexing, and viewer is unaware of the issue.	Other camera channels missed.	Value of evidence reduced, or evidence lost.	Ensure awareness and training is in place. Ensure suitable replay software is used.
31	Lost or skipped frames.	Action or events missed or lost.	Value of evidence reduced or lost.	Ensure awareness and training is in place.

32	Excess information made available to the viewer if they are involved in both the investigative and technical support workflows.	Cognitive bias[11]. Confirmation Bias.[12] non-experts provide opinion evidence on footage which they are not qualified to do or apply incorrect redaction.	Incorrect identification e.g., number plate.	Ensure bias awareness training is in place and working practices are created to minimise inappropriate information being available to the viewer. See Risk 42.
33	Replay Software, performs file conversion and officer is not aware they are viewing a poorer quality copy. Including those players within DEMs, DEAMS and DAMs systems.	Drop in resolution, compression, lost frames, frame rate effects and loss of metadata.	Value of evidence reduced or lost.	Ensure awareness and training is in place. Validate viewable quality when possible, where data is required for further identification/processing.
34	Aspect ratio is incorrect.	Individuals' features or build appear changed.	Affects ability to recognise individual. Could be implied it was deliberate morphing to be a better 'match'. Limits options for further analysis.	Ensure awareness and training is in place.
35	Lack of player functionality, missing Replay Software.	Viewer not aware that audio is present.	Value of evidence reduced or lost, or potential audio	Forces to invest in up-to-date equipment/software.

[11] FSR-G-217, Forensic Regulator Guidance, Cognitive Bias Effects Relevant to Forensic Science Examinations

[12] FSR Regulatory Notice 01/2019 Image Enhancement and Image Comparison: Provision of Opinion

			evidence not realised.	
36	Masking /redaction incorrect, for either still or moving images.	Fails to cover correct people/information. Very high risk and falls into the editing/conversion category.	Vulnerable individuals are inappropriately identified to suspect including potentially undercover officers/test purchasers.	Clear guidance and working practices to ensure this goes through an accredited process where validated systems are not available.
37	Viewer unaware of audio recording that has been captured alongside video.	Actions or events missed.	Value of evidence reduced.	Ensure awareness and training is in place.
38	Automated systems may not identify or recognise content due to limitations of software and data.	Actions or events missed.	Value of evidence reduced and potential missed opportunities.	Ensure awareness is in place around system limitations and periodic verification is in place for software tools.

Evidential Preparation: - Following the CPS, NPCC, HMCTS and FSR guidance				
Ref	**Cause**	**Event/effect**	**Impact**	**Mitigation**
39	Force decides not to have a dedicated service for court preparation of digital evidence.	There is no specialist preparation service.	Excess submissions on non-specialist roles in an unmanaged way resulting in inconsistency. Value and quality of evidence reduced, and professionalism of force brought into	Ensure the issue is understood clearly at strategic level. Force and national guidance and working practices are followed.

			question and will affect public confidence in the police/CJS.	
40	Footage challenged in court (e.g., change of plea, story) late request made of video unit/Judges orders.	Timescales unable to be met by unit due to current workload/tasking.	Case delayed/rearranged/ lost. Non-compliance with SC Code / PoFA	Ensure SLA is in place to provide urgent service.
41	Processes challenged in court.	Further work required following accredited processes. Non-compliance with SC Code / PoFA	Case lost/delayed/rearranged. Value and quality of evidence reduced, and professionalism of force brought into question and will affect public confidence in the police/CJS.	Clear guidance and working practices to ensure this goes through an accredited process where validated systems are not available.
42	Storyboarding/Selection of footage is criticised.	Cognitive bias or acting as an investigator not an expert.	Case is lost, criticism of bias in that case, but potential for previous cases too.	Clear SIO policy / direction. Around bias and impartiality. National CollegeLearn (formally MLE) Understanding Unconscious Bias Pt1-2 course[iii] and Introduction to Investigations v1.0 course[iv]
43	Further file conversion for court playable systems.	A quality drop in the image/footage put to the Trier of Fact (judge/jury).	Case is lost as Trier of Fact (judge/jury) cannot see features.	Ensure the issue is understood and that high-quality viewing

				equipment is available if needed.
44	Incorrect file conversion for court playable systems.	That critical incident or part of evidence (e.g., knife in suspect's hand) is not visible on court version.	Could significantly reduce the value/impact of CCTV presented in court and weaken prosecution case. Also, interpolation and concatenation effects if it involves being reprocessed or over processed.	Ensure there is a clear understanding and auditability of what systems do to image quality, and that high-quality viewing equipment is available if needed.
45	Incorrect capture hardware/software, low CPU/GPU performance, conversion of non-standard/variable frame rate.	Dropped frames in converted video.	Evidence lost during playback at court. Jury unable to review material as it was replayed in court.	Ensure the issue is understood and that high-quality viewing/capture equipment is available if needed.
46	Incorrect capture, conversion, or processing settings.	Incorrect aspect ratio, cropping of relevant detail, loss of detail by resizing or compression.	Value of evidence reduced or lost during playback at court.	Ensure the issue is understood training provided and that high-quality capture/viewing equipment is available if needed.
47	Intentional or unintentional changes to play back speed during processing.	Alters viewer perception of event.	Evidence misrepresented at court.	Ensure awareness and training is in place.

49	Using pre-set templates in editing software.	Inappropriate menus/animation/content on conversion. Lack of corporate approach to graphics and presentation tools.	Value of evidence reduced, and professionalism of force brought into question	Ensure awareness and training is in place.
50	Positioning of mask incorrect, improper interpolation, mask used that can be reversed by processing (e.g., Gaussian blur).	Identity of protected subject is revealed.	Sensitive or vulnerable individuals identified at court.	Ensure awareness and L2/3 training is in place.
51	Irregular framerate, poor syncing by user.	Videos displayed side-by-side lose synchronicity, audio out of sync with video	Value of evidence reduced during playback at court.	Ensure awareness and training is in place.
52	Compression of video during conversion to new format (e.g., to MPEG-2 DVD video).	Loss of detail dependent upon level of compression.	Value of evidence reduced. Material displayed incorrectly during playback at court.	Ensure awareness and training is in place.
53	Filters or processes incorrectly applied at any stage.	Detail lost, artefacts introduced, or events misrepresented.	Value of evidence reduced during playback at court.	Ensure awareness and training is in place.
54	Audio not detected or lost during processing or replay.	Audio does not present in converted copy.	Evidence lost during playback at court.	Ensure awareness and training is in place that highlights the importance of ensuring court systems are capable of replaying and converting audio.

55	Use of non-validated redaction systems to remove personal data (visual and audible)	Fails to affectively redact people/information. Very high risk and falls into the editing/conversion category.	Personal data / vulnerable individuals are inappropriately identified and contravenes GDPR / DPA.	Clear guidance and working practices to ensure this goes through an accredited process where validated systems are not available.

The following general principles must apply when presenting expert opinion in relation to image enhancement and/or image comparison when the images are derived from video footage.

Principle 1: The evidence containing opinion must be admissible in this jurisdiction as expert evidence

Principle 2: The person proposing to give opinion evidence must be an expert in all relevant aspects they intend to give an opinion on.

Principle 3: The person giving evidence must comply with all legal obligations including setting out limitations on the evidence. For forensic science practitioners working in the Criminal Justice System these include, but are not limited to, those set out in the Regulator's publication Legal obligations https://www.gov.uk/government/collections/fsr-legal-guidance

Principle 4: If the expert's opinion relies on the results of any method the report shall take proper account of matters such as the degree of precision or margin of uncertainty, affecting the accuracy or reliability of those results.

Evidential Storage and Transfer: - Following the CPS, NPCC, HMCTS guidance				
Ref	**Cause**	**Event/effect**	**Impact**	**Mitigation**
56	Force decides not to have a dedicated Digital Asset Management or Digital Evidence Management System.	There is physical storage and no secure server or cloud-based evidence store.	Digital evidence stored in an unmanaged way resulting in inconsistency. ICO Non-compliance with GDPR/DPA. Increased risk of data loss/ICO fines. Non-compliance with SC Code / PoFA. Public confidence in the police or CJS reduced.	Ensure the issue is understood clearly at strategic level. Force and national guidance and working practices for data sharing are followed.
57	Digital Asset Management or Digital Evidence Management System automatically converts footage upon upload.	Potential distortion and degradation of original evidence artefacts introduced, or events misrepresented.	Incorrect aspect ratio, time stamps, replay speed, lost frames/cameras lead to value of evidence being reduced during playback at court. Inability to perform further forensic analysis. Investigators unaware of potential errors.	Ensure the issue is understood clearly at strategic level. Systems validated against end user requirements.
58	Ingestion into a Digital Asset Management or Digital Evidence Management System does not detect or	Loss of camera views / evidence due to proprietary formats not being recognised.	Case lost, delayed, rearranged. Value and quality of evidence reduced, and professionalism of force brought into	Clear guidance and working practices to ensure this decoding goes through an accredited process where validated

	recognise multiplexed video streams.		question and will affect public confidence in the police/CJS.	systems are not available.
59	Ingestion does not detect or recognise audio streams within video.	Loss of evidence and events misrepresented.	Evidence misrepresented at court.	Ensure the issue is understood clearly at strategic level. Systems validated against end user requirements.
60	Digital Asset Management or Digital Evidence Management System does not meet standards or lacks validation.	Investigators unaware of potential errors in data handling and misrepresented evidence. Lack of audit trail/authentication.	Case lost, delayed, rearranged. Value and quality of evidence reduced, and professionalism of force brought into question and will affect public confidence in the police/CJS.	Ensure the issue is understood clearly at strategic level. Evidential storage standards to be followed.
61	Remote upload of data via public portals or similar online systems *refer to DAM/DEM issues.	Lack of authentication, potentially pre-processed data received incorrectly. Potential for fake news videos being submitted.	Incorrect aspect ratio, time stamps, replay speed, lost frames/cameras lead to value of evidence being reduced during playback at court. Inability to perform further forensic analysis. Investigators unaware of potential errors.	Ensure the issue is understood clearly at strategic level. Systems validated against end user requirements.

Recovery activities by level

Level 0:

- Third-party requested with SOP in place.
- Remote network connection with established process and SLAs / SOPs in place.
- Remotely hosted with established process and SOPs in place.
- USB provided by third-party (being cognisant of authenticity).
- Original Flash media retained, no requirement to operate the machine.
- Data provided by third-party on optical media (being cognisant of authenticity).

Level 1:

- Remote network connection with no established process if simple, otherwise escalate to level 2.
- Remotely hosted with no established process and SOPs in place.
- Retrieval via USB connected device.
- Retrieval via flash media, requiring operation of the device.
- Retrieval via optical media, requiring operation of the device.
- Removal of device (escalate to L2-3 where complexity exceeds competence).

Level 2:

- Remote network connection with no established process if escalated from level 1.
- Retrieval via USB connected device if escalated from level 1.
- Direct network connection.
- Data extractable directly from a caddied hard drive only.

Level 3:

- Retrieval from corrupted media.
- Data extracted directly from the hard drive.
- Any of the above processes carried out in a laboratory environment.

Dependent on valid method

Unrequested third-party submission (e.g., dashcam submission or file e-mailed as attachment.)

Links to relevant documentation:

Home Office Surveillance Camera Commissioners Code of Practice

Home Office DSTL NPCC Digital Imaging and Multimedia Procedure V3.0

Home Office DSTL Recovery and acquisition of video evidence V3.0

College of Policing CCTV Training

College of Policing Authorised Professional Practice for CCTV

Biometrics and Surveillance Camera Commissioner

Forensic Science Regulator Statutory Code

Forensic Science Regulator Documentation and Legal Guidance

Criminal Procedure Rules and Criminal Practice Directions

College of Policing First Responder Op Modify Course

ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

NISTIR 8161r1 Recommendation: CCTV Digital Video Export Profile – Level 0 (Revision 1)

---

[i] Forensic Units is used in this document to cover forensic science providers of all sizes including small teams or even sole practitioners carrying out the forensic activity and is therefore not limited to a video unit, imaging unit etc.

[ii] "Methods such as recording the screen using Body Worn Video devices or camera phones are poor practice as they do not capture the original data. This will result in a significant drop in image quality, compromising the value of the imagery and making further analysis difficult or impossible. These methods are only to be used as a last resort where all other options have been exhausted or where there is a present and immediate risk of harm to person. Authorisation must be obtained from the SIO and documented, and a copy in the native format must then be obtained, with a request made to level 1, 2 or 3 trained staff.

[iii] Understanding Unconscious Bias. This CollegeLearn (formally MLE) e-learning package provides key information on what unconscious bias is. It includes videos and an aide memoir regarding the common types of biases and examples of how they can be manifested.

[iv] Introduction to Investigations course. This module will enable personnel whose actions or inactions may have a positive or negative impact on an investigation, to possess and use the knowledge, understanding and skills to conduct an initial assessment of the situation and consider the best approach as a first contact. They will also be able to explain how personal attitudes, values and biases can impact on an investigation and the importance of vulnerable people being appropriately supported. Learners will be able to describe the law, policy and guidance in relation to victims and witnesses, the initial response involving digital devices, the evidence that may be obtained during an investigation and the processes for managing the evidence retention and provision of materials during an investigation.

Glossary

BSCC	Biometrics and Surveillance Camera Commissioner
CPIA	Criminal Procedures and Investigations Act
DPA	Data Protection Act
DSTL	Defence Science and Technology Laboratory
FSR	Forensic Science Regulator
GDPR	General Data Protection Regulation
NPCC	National Police Chiefs Council
PoFA	Protection of Freedoms Act
SAI	Senior Accountable Individual
SLA	Service Level Agreement