

CCTV & DIGITAL IMAGES

POLICY & PROCEDURE

OFFICIAL

Government Security Classification Scheme	<i>Policy section:</i> OFFICIAL - Force website approved <i>Procedure section:</i> OFFICIAL - Force website approved
Department of Origin	Force Intelligence Bureau (FIB)
Policy Holder	Det Chief Superintendent Force Intelligence Bureau
Policy Author	Det Insp Andrew Ford / A/D/Sgt Neil Rawley
Related Information	CCTV College of Policing PACE – Code D Framework-Video-Evidence-v3.5-2025.pdf Digital investigations: Digital imaging and multimedia procedure - GOV.UK Recovery and acquisition of video evidence - GOV.UK Protection of Freedoms Act 2012 ECHR Home Police and Criminal Evidence Act 1984 Code of Practice Laboratory Accreditation - ISO/IEC 17025 Data Protection Act 1998 Regulation of Investigatory Powers Act 2000 (RIPA) - GOV.UK Public Sector Equality Duty: guidance for public authorities - GOV.UK Body Worn Video Policy & Procedure Physical and Digital Evidence Retention Model and Review Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice 004-2024-npcc-cctv-portfolio-webinar-october-2023_redacted.pdf ICT Acceptable Use Policy & Procedure
This Version	1.0
Date Created / Modified	10/03/2026
Date Approved (SMB)	01/07/2026
Review By	01/07/2029

Contents

Policy	4
Precis	4
National Context	4
Rationale	5
Aims	5
Objectives	5
Application and Scope	6
Outcome Evaluation	6
Procedure	7
Version History	7
1. FIB Visual Evidence Unit	7
1.1 Role of the Police Visual Evidence Unit (VEU)	7
1.2 How to task the Visual Evidence Unit (VEU)	8
1.3 Mandatory Training & Competence	9
1.4 Forensic Science Regulator Act (FSR Act)	11
2. Retrieval	12
2.2 First response protocol	12
2.3 How to Note the Correct Time on the CCTV System	12
2.4 How to Note the Overwrite Period	13
2.5 Secondary Capture	14
2.6 Witness Statements	14
2.7 Making the appropriate notes when the footage is not relevant	15
3. Copying CCTV at premises	15
3.1 How much footage must be exported?	15
3.2 Copying analogue footage	16
3.3 Copying digital footage	16
3.4 Viewing the copy at the premises	16
4. Force Technical Resources	16
4.1 FIB VEU Assistance	16
4.2 Police officer assistance	17
4.3 The rights of Police Staff to recover evidence	17
4.4 Submitting footage to the CCTV Investigation Unit for editing	17
5. Labelling, Sealing & Evidence of Continuity	18
5.1 Evidence Bags	18
5.2 Depositing evidence	19
5.3 Sanitisation of USB/HDD devices	21
5.4 Maintaining evidence continuity / tracking	23
6. Key Roles and Responsibilities	24
7. The viewing of CCTV stills	24
8. CCTV Prosecution Evidence – Media Format	24
9. Storage	24
9.1 Cloud based storage	25
9.2 VHS Tapes	25
10. Mobile CCTV /Overt Video Evidence gathering / Body Worn Video	25

11. Retention & Disposal	26
12. Human Rights Legislation	26
13. Data Protection Act 1998	26
14. VEU - Security Policy.....	26
15. Protection of Freedoms 2012 (CCTV Codes of Practice: Aug 2013).....	27
16. Digital Image Database.....	27
16.2 <i>How to Access the DID.....</i>	27
16.3 <i>Request Still to be added.....</i>	28
16.4 <i>How to view suspects on the DID.....</i>	29
16.5 <i>Facial Recognition</i>	29

Policy

Precis

This policy is current as of July 2026 however will require further updates due to FIB VEU Estate moves, Changes due to Case Management tasking & reporting software and impending ISO Accreditation requirements.

The proliferation of CCTV, Digital Image systems & Audio systems, in law enforcement, local authority, commercial environments and domestic settings presents Merseyside Police with complex challenges. We are committed to ensuring that, where these systems are installed, their potential for detecting crime and gathering intelligence is maximised.

Historically, the seizure of such CCTV footage and the subsequent process of obtaining and managing images from that footage were not subject to any statutory legal control. With the implementation of the Data Protection Act 1998 and the subsequent publication of the Codes of Practice 2000 relating to that Act, for the first time a legally enforceable set of standards applicable to the collection and processing of images has been formalised. Further statutory control in the form of the Regulation of the Investigatory Procedures Act 2000 (RIPA) and the Human Rights Act (ECHR) which came into effect in October 2000, further Forensic CCTV Codes of Practice issued 19th May 2025, underpinned by the Freedoms Bill 2012, now have significant relevance to the handling of CCTV surveillance and its associated matters.

National Context

Authorised Professional Practice (APP) is produced by the College of Policing as the official source of professional practice on policing. All officers and staff are expected to have regard to APP in discharging their responsibilities. Essentially, our “policy” is to comply with APP as it develops to cover all areas of policing.

[CCTV | College of Policing](#)

The value of closed-circuit television (CCTV) cannot be overstated. Images and audio from CCTV footage play an important role in detecting crime, identifying potential witnesses, identifying and/or eliminating suspects, and identifying potential investigative opportunities, such as event timelines and further CCTV sources.

CCTV allows evidence to be presented in a unique way, letting the courts and jurors visualise aspects of the crime being described. Studies into outcomes using CCTV evidence demonstrate its importance and its direct benefits to crime investigation and achieving justice outcomes.

CCTV can also be a deterrent to potential offenders. It helps to reassure the public, protecting businesses, vulnerable premises and national facilities. It helps public authorities to manage ongoing incidents and is a useful tool when risk assessing scenes.

The Forensic Science Regulator (FSR), working closely with the National Police Chiefs' Council (NPCC), has developed quality standards for the recovery and processing of footage from CCTV and/or video surveillance systems (VSS).

These standards must be followed by all Officers & Staff regardless of role. Mandatory College of Policing training underpins knowledge & ability.

Rationale

The collecting, retrieving, handling and processing of CCTV, Digital & Audio material has undergone significant professionalisation since the publication of the CCTV and Digital Images Policy in September 2016. The process is now considered a Forensic Discipline and is part of the Forensic Science Regulators codes of practice bringing it in line with all other Forensic disciplines. Officers & staff must be trained to appropriate levels as defined by the College of Policing and handle all media in line with their competence & nationally agreed frameworks.

Aims

The main aim of this policy is to establish minimum standards for all Merseyside Police Depts/Units that are engaged or have an interest in the acquisition & processing of CCTV, Digital & Audio Media.

The policy is underpinned by procedures designed to provide clear, definitive and unambiguous direction for all those involved in its deployment and use in the Criminal Justice system.

Objectives

A broad objective is to make best use of all CCTV, Digital & Audio Media providing best evidence in support of Positive Outcomes.

More specific objectives are to:

Ensure compliance with the Forensic Science Regulator Statutory Codes of Practice. This is measurable through UKAS accreditation of FIB Visual Evidence Unit. Adherence with national framework, competency and standards will ensure accreditation is achievable.

Improve quality. By following Frameworks and National standards evidence will be admissible supporting Criminal Justice partners. Improved technology and processes will ensure evidence is gathered, stored, processed, and shared securely. Through training & engagement officers and staff will recover media correctly and in adherence with all regulations.

Ensure fairness and impartiality. All processes involving personal data & biometric data should be proportionate, legitimate and necessary. National guidance held within frameworks should be adopted & followed. Retention and deletion of data should be carried out in adherence with CPIA and other Force guidelines.

Application and Scope

All police officers and police staff, including the extended police family and those working voluntarily or under contract to Merseyside Police must be aware of, and are required to comply with, all relevant policy and associated procedures.

This policy applies particularly to those officers and staff employed within Depts / Units that are main users of CCTV, Digital & Audio Media. These include, but aren't limited too:

- FIB Visual Evidence Unit
- Centralised Crime
- Centralised Public Protection
- Neighbourhood Policing
- Proactive Policing
- BCU Response
- Major Incident Team
- Burglary Investigation Team
- Drugs Investigation Team
- Priority Crime Team
- CMU
- Licensing Unit
- Safety Camera Enforcement
- Forensic Imaging Unit
- Force Operations
- Criminal Justice
- CSD
- Matrix Protective Services
- Eagle Eye
- TSU
- PSD

The Chief Officer lead for CCTV & Digital Images is the Assistant Chief Constable responsible for Force Intelligence Bureau & Investigations.

Outcome Evaluation

Outcomes should reflect specific objectives and be measured against these objectives on a routine annual basis.

Details of UKAS accreditation visits, recommendations and results should be published.

Any errors or findings within laboratory setting shall be raised as a non-compliance and investigated thoroughly with results available.

Community engagement unit are sighted and appraised of all new & emerging technology that processes personal & biometric data.

Procedure

Version History

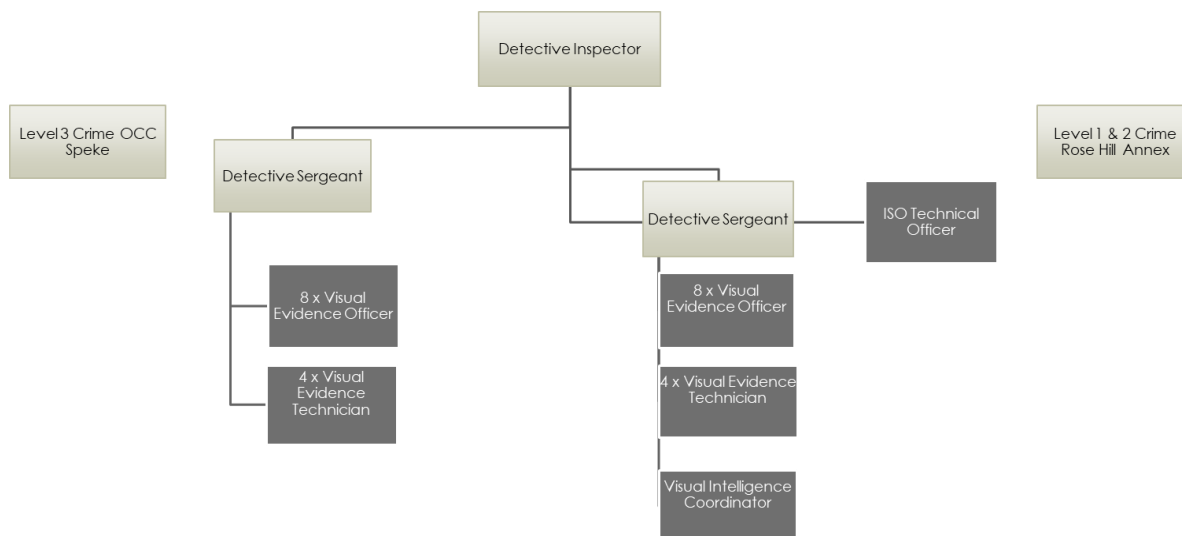
Version Number	Date	Detailed rational behind amending/updating policy or procedure.	Policy Owner Details	Policy Author Details
1.0	02/03/2026	Initial draft	D C/Supt FIB Graeme Robson	D/inspector Andrew Ford A/D Sgt Neil Rawley

1. FIB Visual Evidence Unit

1.1 Role of the Police Visual Evidence Unit (VEU)

- 1.1.1 The Visual Evidence Unit (VEU) is responsible for the lawful acquisition, management, analysis and presentation of visual material for policing and criminal justice purposes. This includes CCTV footage, body worn video, mobile phone recordings, dashcam footage and other digital visual and audio media.
- 1.1.2 The Unit ensures that visual evidence is obtained and handled in accordance with relevant legislation, codes of practice and force policies, including data protection, privacy and evidential integrity requirements. All material is managed securely to preserve its authenticity and continuity, enabling it to be relied upon in criminal investigations, court proceedings and oversight processes.
- 1.1.3 The VEU supports investigations by reviewing visual material to identify persons, vehicles, locations and sequences of events, and by producing evidential outputs such as still images, clips, enhancement work and multi-media compilations where appropriate. Any processing of footage is conducted using approved methods that do not compromise the original evidential value.
- 1.1.4 The Unit also provides expert advice to officers and staff on the evidential use of CCTV and other visual media, including best practice for retrieval, submission, storage, retention, disclosure and redaction. It works closely with CCTV system owners, investigators, prosecutors and the courts to ensure visual evidence is proportionate, relevant and lawfully used.
- 1.1.5 In the context of CCTV systems, the Visual Evidence Unit plays a key role in ensuring footage is accessed only for legitimate policing purposes, that requests and disclosures

are properly recorded, and that the rights of individuals captured on camera are respected.



1.2 How to task the Visual Evidence Unit (VEU)

1.2.1 Niche

The Visual Evidence Unit can be tasked to assist with numerous activities. To make a request, the officer should open the OEL entry on the requested Niche occurrence. A new entry should be added and using a CCTV template from the list, select the most appropriate CCTV template and fill in all the applicable sections. Below is a list of the 4 relevant templates available.

- **CCTV 1 – Recovery Request.** The officer should attend location and attempt to download footage using their Level 0 and Level 1 CCTV training. Should the officer not be able to retrieve the footage, efforts should be made to speak with a member of staff from VEU to try and resolve the issue over the telephone. Should this not be possible, then a request can be made, filling in all details and reason for VEU attendance. Should there not be enough details or efforts to recover this footage, the request may be rejected by a VEU supervisor.
- **CCTV 2 – Processing Request.** Any processing requests which can be any of the following:-
 - Audio redaction,
 - Visual redaction,
 - ABE edit,
 - Copy or converting any footage,
 - CCTV compilation request,
 - SAR,
 - Wirral CCTV download etc.

- **CCTV 3 – Custody Request.** Officer can request footage from any Merseyside Custody suite. Full details are required, including description of nominal, date and times when arrive at location, and reason for request. Officers cannot request footage for a ‘just in case’ scenario.
- **CCTV 4 – Body Worn Video Request** – Request for any edit or redactions on any BWV. Requester needs to provide full details of what is required. Any redactions need to contain exact detail and cannot use vague requests i.e. remove any personal details but should be precise information i.e.: remove nominal name at 16:12:02 – 16:12:05.

1.2.2 Once the OEL entry has been completed, a task should be submitted to *Visual Evidence Unit. The task should be marked Low/Medium/High pending on type of request. The task should have a brief description of what the task is and include any target dates that have been requested.

1.2.3 Should the request be urgent, it is recommended that the requester contact the Visual Evidence Unit to highlight the urgency. During office hours 07:00 – 19:00 Monday to Friday look for the duty VEU Detective Sergeant or use the Skype Visual Evidence Unit contact number 777 7793.

1.3 Mandatory Training & Competence

1.3.1 CCTV Level Zero Op Modify

Operation Modify (also known as Op Modify) helps new and serving officers, police staff and volunteers to acquire the digital skills they need to undertake investigations effectively. Op Modify consists of 15 episodes on College Learn (you will need to log in).

This training package is mandatory and provides basic learning in relation to Digital Disciplines. Those who complete Op Modify are competent to receive Digital & Audio Media provided to them by the proprietor. This can be a physical exhibit or digital link such as NICE Investigate Business or Citizen request.

Put your digital investigative skills to the test with [Operation Modify | College of Policing](#)

CCTV First responder's protocol

What you need to do

- **Carry out checks** (ensure correct date/time of CCTV and camera views required)
- **Record relevant information** (camera views, system information, retention period, system output format)
- **Trained operator available?** Get them to download the footage
- **Trained operator not available?** Retrieve the system password and submit request to trained operator

CCTV First responder's protocol

What you must not do

- **Don't** operate a machine unless you have received the appropriate training
- **Don't** unplug anything
- **Don't** switch the machine off
- **Don't** change the time and date
- **Don't** change any other settings
- **Don't** record the screen with a mobile or body worn video

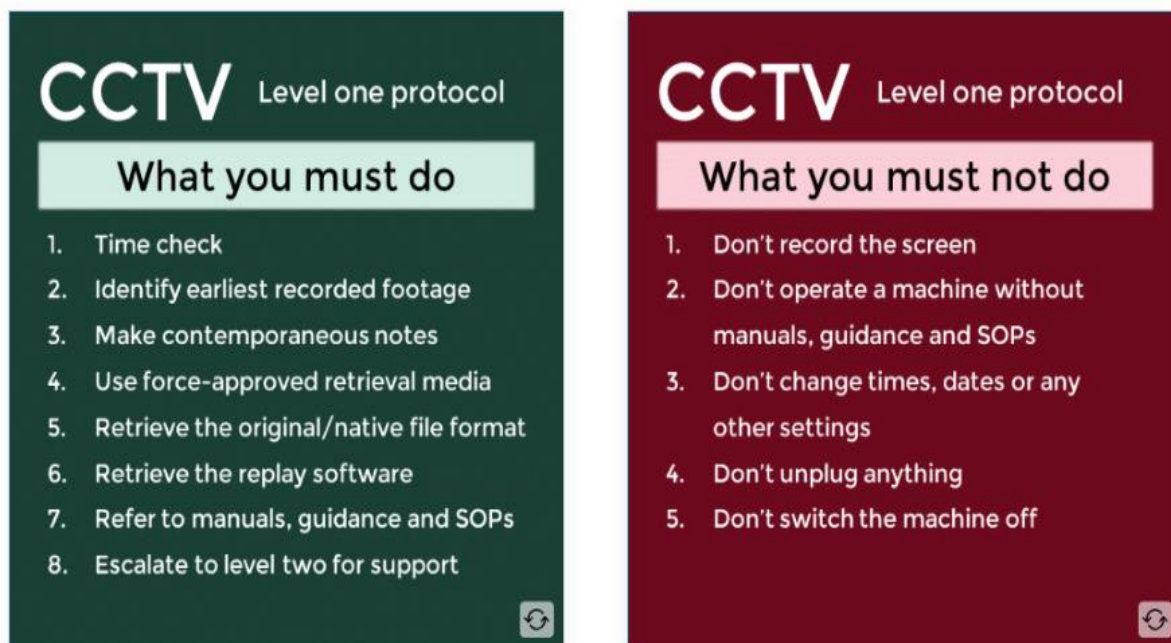
1.3.2 CCTV LEVEL ONE

SEE COLLEGE LEARN FOR CCTV LEVEL 1 TRAINING.

All personnel are required to complete both CCTV 0 Op Modify and CCTV 1 mandatory CCTV training. Those who complete L1 COP training will be competent to download CCTV footage following manufacturer's instructions and correctly record the details.

Staff will have to have completed both CCTV Level 0 Op Modify and Level 1 prior to any request for VEU assistance. VEU assistance is only available for specialist requests.

Further details are available on IForce [Visual Evidence Unit](#) to assist with downloading from different CCTV systems.



CCTV L2 & L3 are not mandatory for Operational Staff at present and are only required for FIB Forensic Science Activity completed within the Visual Evidence Unit.

1.4 Forensic Science Regulator Act (FSR Act)

The Forensic Science Regulator Act 2021 (FSR Act) provided new statutory powers to the Forensic Science Regulator (FSR). The FSR ensures that the provision of forensic science services and activities across the criminal justice system are subject to appropriate scientific quality standards. The FSR code aligns to regulations set by the International Organization for Standardization (ISO). For CCTV, the relevant regulations are BS EN ISO/IEC 17020 (activities in the field) and BS EN ISO/IEC 17025 (activities in laboratories).

A key element to remember is that the FSR has agreed some exemptions to the activities by reducing the requirement for personal accreditation but still following the code. Some front-line activity may be performed by trained and competent staff using standard operating procedures or simple manufacturer intended methods, such as those that the owner would use.

This means at level zero; you can attend to collect footage that has already been downloaded or exported by the owner or operator of the CCTV system.

At level one you must only retrieve CCTV footage if:

- you are trained and competent.
- you use standard operating procedures including the use of manufacturer's intended methods.

Any other retrievals must be escalated to level two or three operatives.

2. Retrieval

- 2.1.1** When Officers/Staff attend an address to retrieve footage, they should firstly ascertain what the type of system is and how the CCTV is recorded, i.e. onto a local storage/Hard Disk Drive or Cloud storage based.
- 2.1.2** The officer should be able to utilize their knowledge from Level 0 and Level 1 CCTV training to retrieve the footage they require. Part of this training is using the user manual for the CCTV DVR system.
- 2.1.3** Further guidance available on the VEU IForce site [Visual Evidence Unit](#).
- 2.1.4** Footage can be provided by uploading to a cloud-based storage or an external storage device i.e. sanitized USB.
- Officer should make full notes at location. Notes should include the following:
 - Exhibit Reference
 - Description of exhibit
 - Location
 - Date/Time Seized
 - Cameras downloaded.
 - Earliest recorded date
 - Parameters seized (Date/Time)
 - Calibration (System and Actual Time) – Calibration being Hour:Minute:Second). Also note if fast/slow and if GMT/BST
- 2.1.5** These details should be recorded on your Pronto device or in your Pronto ePNB.
- 2.1.6** If the only method is to export to an external device, then this device should be placed into a CCTV exhibit bag. The bag should be sealed and all details recorded in the fields provided.

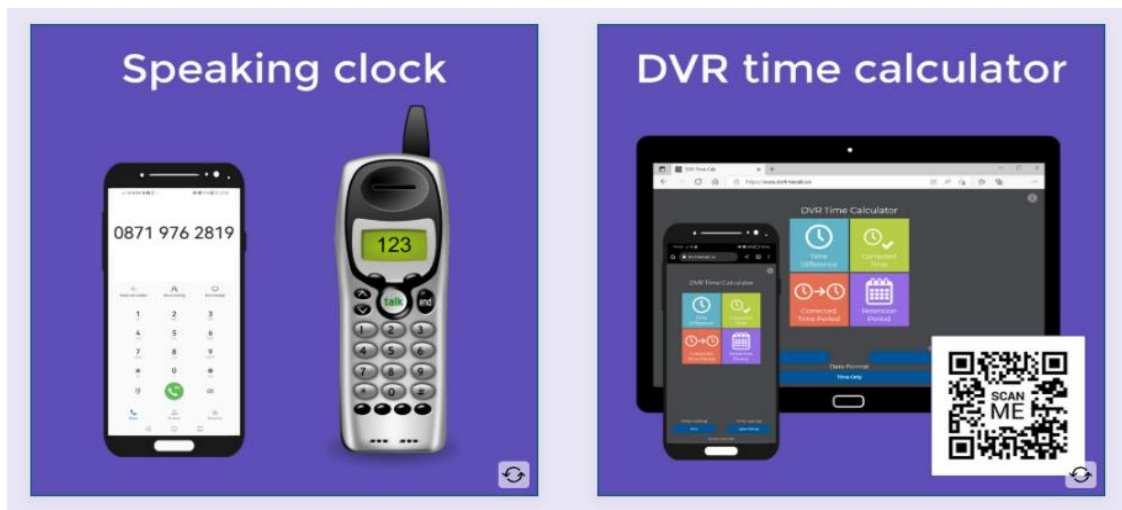
2.2 First response protocol

- 2.2.1** As above – Only deal with what you're competent to do (COP level) and following instruction.

2.3 How to Note the Correct Time on the CCTV System

- 2.3.1** Noting any difference in time calibration is very important part when retrieving footage, even if the footage is a few seconds out. This can play a pivotal role later in an investigation should the accuracy of the footage be challenged.
- 2.3.2** Majority of the time, the system time will be out so a record should be kept showing what the system time is and what the actual time is. The website <http://time.is> can be used to check what the accurate time is. With this, the time calculation can be worked out using <http://dvrtimecalc.uk>, whereby you can enter the system time and actual time this will

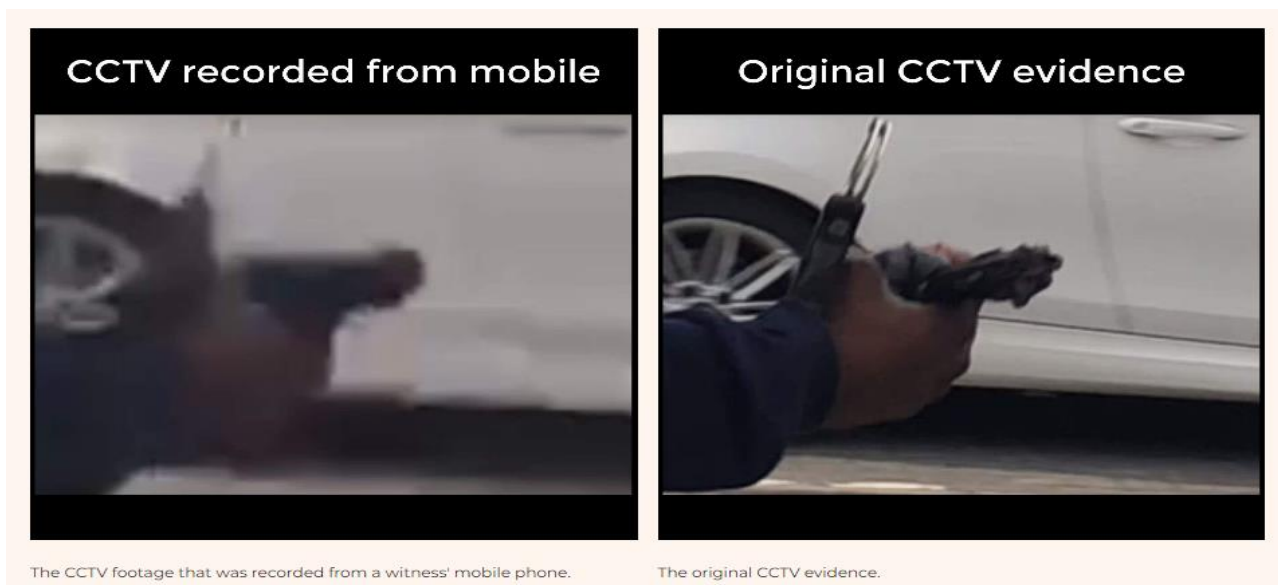
work out the time difference. This application can also be used to calculate any time difference you require when retrieving specific dates and times.



2.4 How to Note the Overwrite Period

- 2.4.1 It is important to note the over-write period of the CCTV system so that officers are aware of how much time they have left to extract Media, before the footage is lost forever. This is particularly relevant if officers need to return after the event to extract additional footage.
- 2.4.2 It is not enough to simply ask the owner what the overwrite period is. You should check this yourself or you can ask the owner if the earliest footage saved on the system can be viewed. The number of days between the date of the earliest recorded material and the date of attendance is the over-write period.
- 2.4.3 This is critical in assessing the level of response required if support is required from the VEU. Once Media is overwritten it is impossible to recover.

2.5 Secondary Capture



ACC Jenny Gilmer - NPCC Lead for CCTV:

“Taking a video or image of CCTV footage on body-worn video or other mobile device may be seen as a pragmatic way to assist with reasonable lines of enquiry whilst waiting on a formal evidential download to be completed. It does however have the potential to create significant procedural difficulties and should only be considered for immediate intelligence purposes only (for example, where there is an immediate threat to life or to facilitate recognition of an offender at large). It must always be followed up with a valid download of the original image data.”

DCC Jim Colwell - NPCC Lead for Body Worn Video:

“It would be welcomed if you could ensure your BWV policy instructs your officers that:

- The use of BWV to capture video or images from any another device is only seen as a last resort in response to immediate intelligence purposes for recognition only.*
- Officers must ensure that if this is done, the original source recording must also be seized and treated as an exhibit in line with current working practices.”*

[Secondary Capture Communications - final.pdf](#)

2.6 Witness Statements

- 2.6.1 The person who retrieves the footage from the CCTV system will need to complete a witness statement to ensure the continuity of the evidence. This person could be the owner of the system, an engineer or the officer/staff member that has seized this footage. The witness statement need only contain the details of what the person did to retrieve the footage. It may only be a few sentences outlining the date, time and how the person exported the footage, for example, downloaded the footage onto a USB device. Any

discrepancies between the time shown on the CCTV system and the actual time of the footage must also be noted in the statement to show the accurate calibration, this should be recorded HH:MM:SS format, stating if fast or slow and also method of calibration i.e. DVR timecalc or Time.is.

2.6.2 The statement should include if the exhibit has been provided to an officer. A disposal statement will be also required to show what the end process was. This can be one of the following:

- Master exhibit booked into Niche Property management system. Exhibit sent to EMU for storage.
- Master exhibit uploaded to NICE. Validation check complete to show the correct number of files were uploaded correctly. Officer to check the files are all viewable. If not, then consideration to task VEU to convert the files and requesting the external device be sent to VEU by EMU.

2.7 Making the appropriate notes when the footage is not relevant.

2.7.1 When investigating volume crime, the officer attending the scene has discretion as to whether the footage available is relevant to the investigation. If the officer attending believes the footage is not of relevance, they must always record the reasons in their pocketbook, Daybook or Pronto as to why they chose not to seize the footage. In cases of serious crime, the SIO will give guidance as to what should and should not be retrieved. If the footage does not meet the requirements of the investigators/SIO, officers must make a note in their pocketbooks as to why the images did not meet these requirements. Poor quality images/footage of incident must be seized. All notes should be added to the Niche OEL.

3. Copying CCTV at premises

3.1 How much footage must be exported?

3.1.1 It will be on rare occasions when several hours' worth of footage (or even several days' worth) will be needed for the purposes of an investigation. As a result, careful consideration will need to be given as to how much footage to export. If officers have not been informed by an SIO as to how much to take, it is best to keep the amount as small as possible. However, officers must liaise with the SIO in order to determine what amount of footage is required for any given investigation. This amount will depend on the nature of the offence, the accuracy of the victim's/witness' account that the incident happened at a particular time and a suitable contingency based on the circumstances. If the overwrite period is correctly noted, officers can return to the premises within this time to extract further footage if the need arises.

3.2 Copying analogue footage

- 3.2.1 In cases where only a small amount of footage is needed, or where a CCTV system does not allow VHS copying, officers can simply remove the VHS tape and secure it as evidence. This can then be converted at the VEU. The original or master tape must be secured. The tape must be wrapped in anti-static bubble before being placed into exhibit bag and exhibited correctly before submitting this to the VEU. Should this not be done correctly, the exhibit will be rejected. An OEL entry and task must be submitted for the VEU to review this request.

3.3 Copying digital footage

- 3.3.1 Unless the CCTV owner is a witness to the incident, officers must decide whether the owner is competent and trustworthy enough to download the relevant footage. This is covered in CCTV Level 0 training. If the owner is unable to do so, and a system engineer is not available to download, then the officer should be CCTV level 0 and level 1 trained and should be able to carry out this task. Should this fall outside of this and require specialist VEU attendance, then a request should be made with details of what is required. The officer will need to provide full details of reason why they were not able to complete this retrieval, as well as recording details to complete the OEL entry. The officer should take photographs to assist the VEU. If the officer does not record enough detail, the request may be rejected by the VEU, and the officer will have to return to the location to obtain the correct details. It is recommended that the officer contacts the VEU whilst at the location, as support may be given via telephone advice.

3.4 Viewing the copy at the premises

- 3.4.1 Before an officer leaves the premises, it is advisable that any exported footage is viewed briefly and checked so as to confirm that the footage has exported correctly.
- 3.4.2 Often CCTV systems do not have the facility to review copies and enquiries should be made for a CCTV retrieval laptop.
- 3.4.3 Failing this, CCTV should be checked on a standalone PC at a local police station, with the footage being viewed via a writeblocker. This being to prevent any loss of data. Footage should never be viewed without a writeblocker, and advice can be sought via the Visual Evidence Unit.

4. Force Technical Resources

4.1 FIB VEU Assistance

- 4.1.1 When officers experience difficulties retrieving CCTV footage, the Visual Evidence Unit may be requested to assist in the retrieval. They may suggest the removal of the hard drive or of the entire CCTV system. Both of these procedures require relevant technical training and must NOT be carried out by officers untrained to do so. A damaged system

may not only jeopardise the retrieval of the footage, but it may also cause huge costs in the form of compensation.

- 4.1.2 In major investigations where a lot of CCTV is to be retrieved in a short amount of time, the Visual Evidence Unit must be contacted as soon as possible. This will enable the VEU to prepare for a large number of requests. In addition, if large geographic locations are to be trawled on a particular day, it may be helpful for members of the VEU to accompany officers as they visit premises. Technical assistance will then be immediately available if needed. In most major investigations, the parameters for the search and retrieval of CCTV footage will be contained within a specific strategy that will have been drafted by the SIO and contained within the policy file.

4.2 Police officer assistance

- 4.2.1 In cases where a police staff member is tasked with retrieving footage; a police officer may need to accompany the member of VEU staff during the retrieval. This is particularly relevant if, for example, there is risk that the owner will not allow staff from the Visual Evidence Unit to remove the hard drive or system, as police staff generally have no power of seizure.

4.3 The rights of Police Staff to recover evidence

- 4.3.1 Police staff from the VEU can only retrieve footage with the consent of the owner.
- 4.3.2 Should a request for VEU to attend an address to seize/retrieve any footage, the requester should make enquiries that the owner of the CCTV system gives consent for the police to attend and for the VEU to recover.
- 4.3.3 Should a warrant be required to seize/download any footage, then VEU staff will need to be added to the warrant and in company with a police officer.

4.4 Submitting footage to the CCTV Investigation Unit for editing

- 4.4.1 Should the CCTV exhibit require any work to be completed by the VEU, then firstly the requester needs to complete a CCTV OEL template using the relevant CCTV template.
- 4.4.2 Once completed, a task should be sent to *Visual Evidence Unit with what is required.
- 4.4.3 The exhibit must be exhibited correctly, utilising the correct packaging and details. Should there be any errors, the exhibit will be rejected and potentially a Non-Conformance will be raised by a VEU member of staff. This will be investigated & resolved internally. The requester will be required to attend the VEU laboratory to correct the error in any event.

5. Labelling, Sealing & Evidence of Continuity

5.1 Evidence Bags

- 5.1.1 Bespoke CCTV exhibit bags have been designed to assist with the correct packaging and recording of data for CCTV retrievals. These bags will be available on Scene Safe, the registered Force supplier. Staff are to refer to local admins and BCU arrangements to order replacement stock.
- 5.1.2 When retrieving CCTV footage, the bespoke CCTV exhibit bags should be completed fully and used to secure the device. Once the exhibit is placed into the exhibit bag, this should be sealed. This can be later opened by the officer to allow them to upload the exhibit to NICE as the master exhibit. The following items can be placed into the CCTV exhibit bags:
- Micro SD/Sd cards
 - Dashcam
 - CD/DVD/Blu-Ray Disc
 - USB
 - Internal HDD
 - External HDD
- 5.1.3 Exhibits should be handled with care. Any exhibit, in particular with moving parts i.e. Hard Drive or delicate items such as VHS tape or mini reels should be wrapped in anti-static bubble before being placed into exhibit bag.
- 5.1.4 Should VEU assistance be required to perform any specialist tasks, the VEU will only accept CCTV that has been sealed in the correct CCTV Exhibit bags and all details correctly entered.

Do Close: Remove backing tape and press seal firmly against a flat surface

CCTV EXHIBIT USE ONLY:

###SERIAL NUMBER / BARCODE###

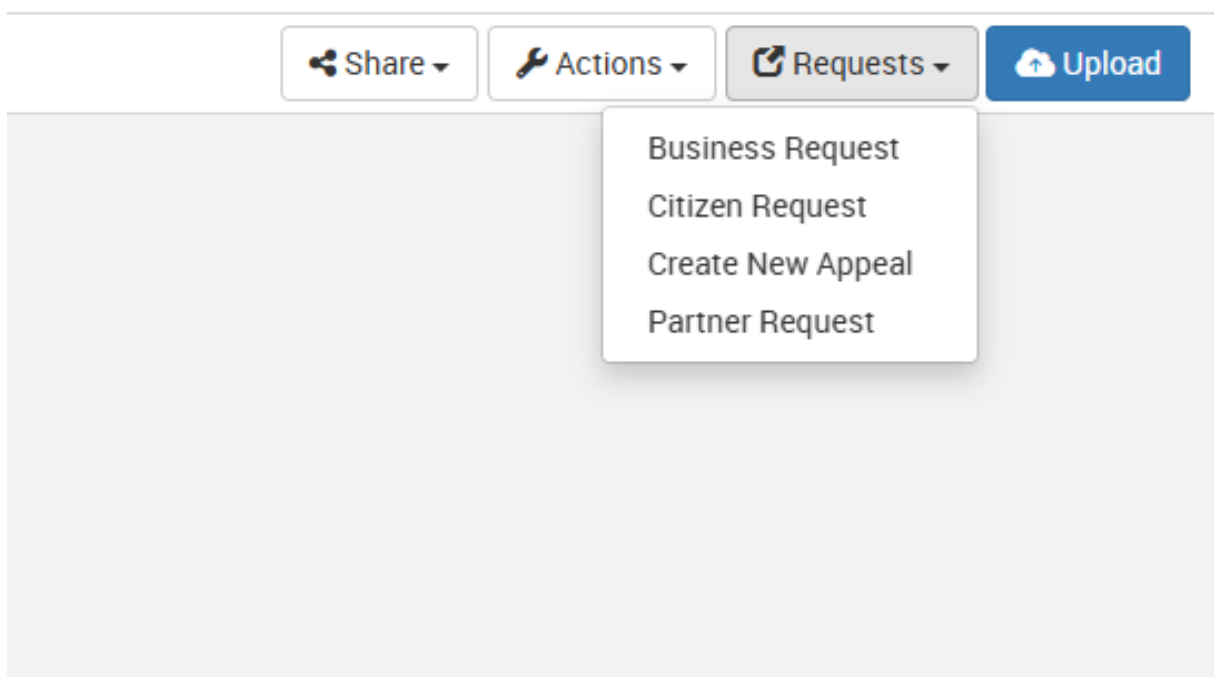
Write using ball point pen

ORGANISATION:	(Continuity Box 1)	
CASE REF NO:	Name/Rank/No. (Block Letters)	
EXHIBIT REF:	Signed	
PROPERTY NUMBER:	Date / Time:	
DESCRIPTION OF EXHIBIT:	(Continuity Box 2)	
.....	Name/Rank/No. (Block Letters)	
.....	Signed	
.....	Date / Time:	
CAMERAS DOWNLOADED:		
.....	(Continuity Box 3)	
.....	Name/Rank/No. (Block Letters)	
.....	Signed	
.....	Date / Time:	
NOTES:		
.....	(Continuity Box 4)	
.....	Name/Rank/No. (Block Letters)	
.....	Signed	
.....	Date / Time:	
EARLIEST CCTV RECORDED DATE:		
.....	(Continuity Box 5)	
.....	Name/Rank/No. (Block Letters)	
.....	Signed	
.....	Date / Time:	
PARAMETERS SEIZED:		
DATE FROM: TIME FROM:	(Continuity Box 6)	
DATE TO: TIME TO:	Name/Rank/No. (Block Letters)	
.....	Signed	
.....	Date / Time:	
CALIBRATION TIMES:		
SYSTEM TIME: (HH:MM:SS)	(Continuity Box 8)	
ACTUAL TIME: (HH:MM:SS)	Name/Rank/No. (Block Letters)	
CALIBRATION: (HH:MM:SS)	Signed	
FAST ☐ SLOW ☐	Date / Time:	
METHOD USED TO CALIBRATE:		
LOCATION DETAIL S:		
RECOVERED/OBTAINED FROM:	LAB USE ONLY:	
.....	LAB REF NO:	
.....	RECEIVED BY:	
.....	RECEIVED TIME/DATE:	
DATE SEIZED: TIME SEIZED:	RECEIVED CORRECT: YES ☐ NO ☐	
SEIZED BY (Name/Rank/No.) (Block Letters):	PHOTOGRAPHED: YES ☐ NO ☐	
Signed	PROPERTY LABEL ATTACHED YES ☐ NO ☐	
.....	DISPOSAL:	

5.2 Depositing evidence

- 5.2.1 The exported CCTV exhibit should be uploaded to NICE as the master exhibit. This should be achieved by uploading the exhibit via a standalone PC at a designated police station. If the footage is on an external device i.e. USB or External HDD, then this must be plugged into the writeblocker.
- 5.2.2 Once the footage has been uploaded to NICE, checks should be performed to make sure the files have transferred over correctly. This can be done by checking the hash value of the original exhibit and NICE copy. Personnel are to check the activity section for clarification.

- 5.2.3 The USB can either be booked into property if still required or can be sanitised and reused.
- 5.2.4 A request for CCTV footage (inc. doorbell, mobile phone, dashcam, etc.) can be sent via a Citizen or Business 'Request' on NICE Investigate. Where the occurrence is known, the request should be created from within the NICE occurrence. In the absence of an occurrence, a request can be made from the REQUESTS section on the home screen, but once received, the recording should be reviewed and either 'Added to a case' or 'Marked for deletion' and the reason provided, whichever is applicable.
- 5.2.5 If the citizen can download CCTV themselves and aware of the guidance within CCTV level 0 training, then a CCTV Citizen request can be made via NICE. You will need to have an email or mobile number from the citizen, where they will receive a NICE request to upload the footage. It is still important that you obtain full details and method on how they will perform this task, and also important information i.e. Time calibration and method of calibration.



- 5.2.6 A NICE 'Business' Request rather than Citizen Request must always be used when engaging with businesses. Where a business is not already registered, the Requestor should send them a new business registration from NICE. Registering businesses is a critical step, as it establishes a reliable record used for future investigations, significantly improving the speed and efficiency of obtaining footage. This is a straightforward but critical process.

New Business request: New Business Registration ☆ Mark as Favorite

Search businesses, contacts and groups *

Type a business or contact name to Search, then click to add as recipient.

Requests

Business	Contacts	Cameras
Registration Request Only		

This request is being sent to you so that you can register with the NICE Investigate Community Portal. **There is no requirement for any footage at this time.**

Pre-registration will assist if you ever become a victim of crime and have digital evidence to submit to the police. It will also assist Merseyside Police with any investigations where it is established that your premises may have CCTV footage relevant to an incident. **This registration DOES NOT give Merseyside Police access to your cameras**, it simply gives Merseyside Police a quick way to request you to review your own footage and upload it if applicable.

Please enter a message to accompany this registration request (optional)

[Create Request](#)

- 5.2.7 When the status of a request sent to a Citizen or Business changes a notification update is shown on NICE, e.g. Sent, or Read. If they respond to the request the status shows 'Completed', and the Requestor is auto emailed to prompt the review and processing. All requests and their status show on the Requests tab on the NICE case.

EVIDENCE	SUGGESTIONS	DETAILS	COMMENTS	ACTIVITY	REQUESTS
CITIZEN - OUTGOING CIT266178 COMPLETED			Created on 7 April 2022, 13:09:49		
CITIZEN - OUTGOING CIT261887 SENT			Created on 3 March 2022, 19:27:51		
CITIZEN - OUTGOING CIT261877 READ			Created on 3 March 2022, 18:30:19		

- 5.2.8 It is essential that all 'completed' requests (i.e. responded to) are reviewed and relevant footage is 'added to case' and irrelevant footage 'Marked for deletion'. It is also important to review any written response provided by the Citizen.

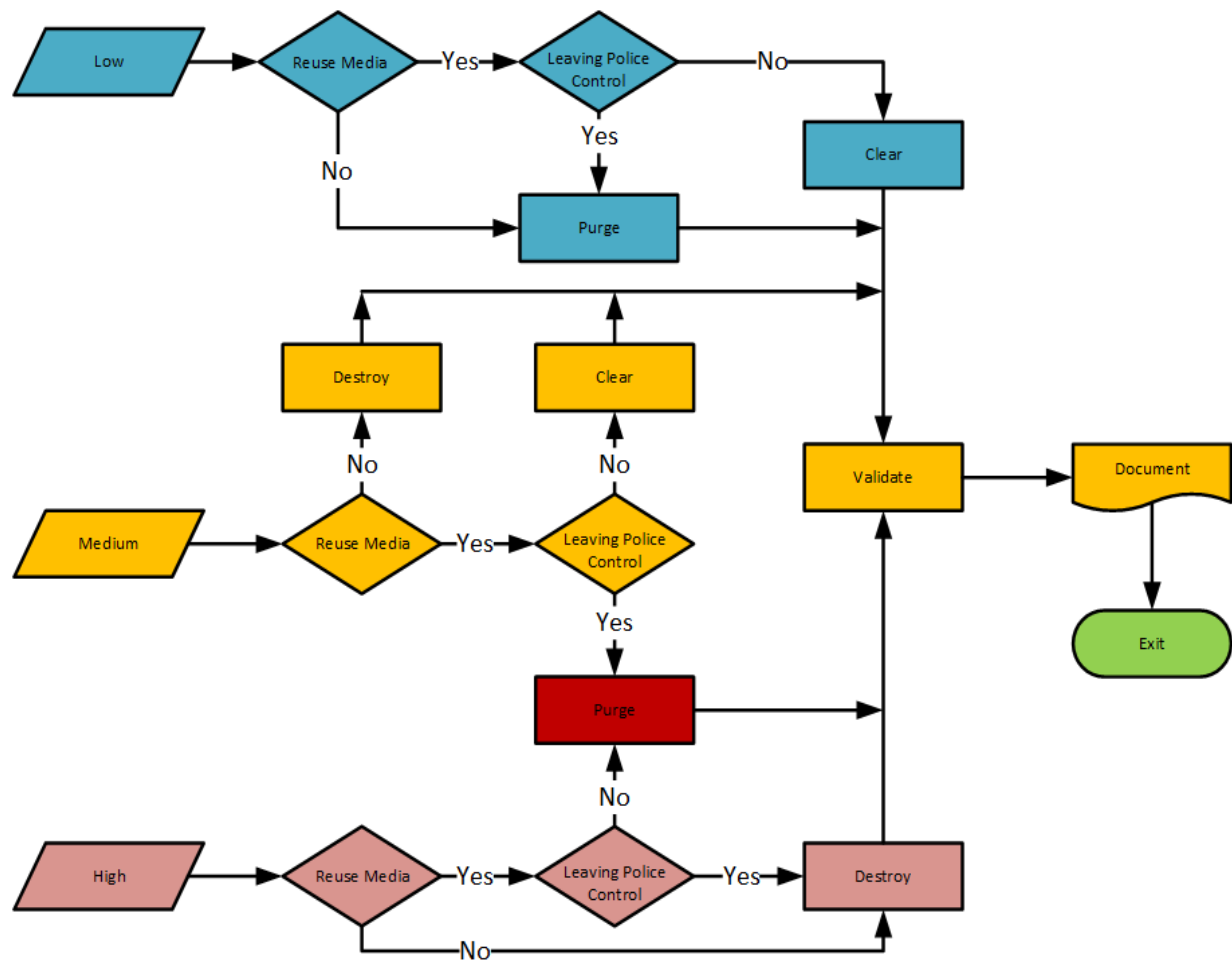
5.3 Sanitisation of USB/HDD devices

- 5.3.1 Once the external medium (USB/External HDD) has been used and no longer required, then this can potentially be sanitised and reused.

5.3.2 Depending on where the storage device is retained, will decide on what process of sanitisation is required.

5.3.3 Below is a flowchart to assist with what method is required. First is to determine if the footage on the device is Low (Official), Medium (Official Sensitive) or High (Secret). Then the officer/staff member needs to decide if the storage device will leave Police Control, i.e. they are keeping hold of the storage device to perform further retrievals. Following this flowchart will inform the officer whether to (physically) destroy, Clear or Purge the device.

- **Clear:** sanitise data in all user-addressable storage locations, protecting against simple non-invasive data recovery techniques, such as those supplied by storage manufacturers to recover accidentally erased files. This is typically achieved using standard Read and Write commands to the storage device and include rewriting with a new value or using a menu option to reset the device to the factory state. This could be achieved using a process such as Full Format on a Windows® machine with an operating system newer than Vista®. This method doesn't work with damaged media or media that is not re-writable. This can be performed on a standalone PC at designated police stations.
- **Purge:** techniques that render data recovery infeasible using state of the art laboratory techniques. In this environment this is likely to involve a 3 or 5 pass erase procedure and is most easily achieved using dedicated hardware. This can only be performed at the Visual Evidence Unit. This can be arranged by either hand delivering to the Visual Evidence Unit at Rose Hill; OCC or can be transported to the Visual Evidence Unit. Please update the OEL with the request and send a task to *Visual Evidence Unit requesting this asset/device to be Purge sanitised. The VEU will complete this task and inform the requester once complete and how to collect the Medium.
- **Destroy:** This requires the physical destruction of the device.



5.4 Maintaining evidence continuity / tracking

- 5.4.1 The recorded media should be uploaded to NICE as the master exhibit. Major Investigation Team exhibits to be maintained as per current SIO policy. Should the transferable media be required to be kept, then this must be correctly booked into the evidential property system on NICHE. The item(s) should be placed into the relevant interim property store within the station, where the exhibit will be sent to the EMU for storage.
- 5.4.2 Should the media be needed to be sent to the Visual Evidence Unit for specialist tasking, then this can be either taken by hand to the Visual Evidence Unit at Rose Hill Annexe or OCC, or a task can be sent to *EMU to move the exhibit to VEU Rose Hill. A CCTV OEL template must be used with what action is required and a task to *Visual Evidence Unit.
- 5.4.3 On receipt of the digital media within the VEU, a staff member will book the exhibit into the VEU store. A VEU supervisor will allocate the CCTV task to a VEU staff member to complete the task.

6. Key Roles and Responsibilities

6.1.1 The Visual Evidence Unit have a major role in the preservation and processing of CCTV evidence and have the knowledge to deal with a wide variety of media formats and codecs, including; VHS, Hi8, Mini DV, CD, DVD, USB, Memory Cards, Hard Drives and full Digital Video Systems including networked installations.:

- Storage of all CCTV data
- Production of copy evidence for court / investigatory requirements in viewable formats
- Production of Images for identification purposes, and producing Bulletins
- Clarification of Images.
- Specialist editing (redaction) for court / interview.
- Seizure / retention / production of CCTV from Council maintained systems.
- Retrieval of CCTV from Custody Suites/Police Stations.
- Retrieval of CCTV Data from DVR systems both on site and from seized systems.
- Interrogation of Hard Drives for CCTV data.
- Weekend call out for major incidents authorised by FIM/Duty DCI.
- Audio enhancements
- Visual enhancements
- Visual redactions

7. The viewing of CCTV stills

7.1.1 The viewing of CCTV stills on the Digital Imaged Database must be conducted in an effective controlled manner, with transparency of process to support any positive identification outcome. See Section 16 for full process.

8. CCTV Prosecution Evidence – Media Format

8.1.1 Primary method for providing media should be digitally through NiCE Investigate Share CJ & MG0, in line with the national blueprint and MOU.

8.1.2 In exceptional circumstances such as business continuity or significant file size CCTV evidence for Crown Court can be supplied via DVD/Blu-Ray or external device i.e. USB/External HDD. SIO should be aware, and this process authorised.

9. Storage

If CCTV footage is downloaded onto a USB/External Hard Drive as a Transferable Medium, this footage will need to be stored as a master exhibit.

9.1 Cloud based storage

- 9.1.1 NICE should be considered as the primary location to store evidential footage (*'relevant' used and unused material*). This footage should be uploaded to NICE utilising VEU support or one of the force ingest stations that have been set up throughout the force. A writeblocker should be used to prevent the footage from being wiped or damaged and then uploaded to NICE. The accuracy of the data can be checked by checking the Hash Values of both the footage on the transferable Media with the Hash value of the footage on NICE. This should be documented to confirm that both match and no errors. The OIC should then decide whether to keep the original external device and book this in as property, or if not then follow the sanitation flow chart within this policy.

Note as per 5.4.1 - Major Investigation Team exhibits to be maintained as per current SIO policy.

- 9.1.2 Whilst in decline, the use of videotapes to record CCTV footage, is still a medium that the police service has to manage which can pose storage issues.

9.2 VHS Tapes

- 9.2.1 VHS tapes must be stored above basement level, in a secure non-metallic area, away from magnetic emissions, in temperatures between 15-25° C, 40%-60% humidity. Fire extinguishers must be available with signs displaying danger of noxious fumes and the fire service given plans of the storage area. CD/DVDs must be stored in similar conditions as those of VHS tapes. The fire service advise that CD/DVD's when burning give off thick black acrid smoke, noxious fumes, intense heat and have a rapid fire spread. The Fire service must be informed of the location of storage.
- 9.2.2 ACPO surveillance guidelines also recommend all tapes used in evidence should be kept for a period of not less than 7 years. It is recommended that the incident only (as confirmed by the CPS) should in the case of VHS tapes, be transferred to DVD/CD and the original recording returned to the copyright owner (CPI Act 1996 Sec 2.14). This process will reduce the storage burden on the force.

10. Mobile CCTV /Overt Video Evidence gathering / Body Worn Video

- 10.1.1 There are a number of mobile CCTV systems in use by the organisation that are a valuable asset when used in a legal, justified and proportionate manner.
- 10.1.2 With regard to Body Worn Video, separate Force guidance is signposted at the below shown link.

[Body Worn Video Policy & Procedure](#)

- 10.1.3 Live facial recognition, Officer Initiated facial recognition and retrospective facial recognition are covered in separate policies held on IForce.

[Live Facial Recognition Policy & Procedure](#)
[Retrospective Facial Recognition Policy & Procedure](#)

11. Retention & Disposal

- 11.1.1 All CCTV & digital media evidence must be retained / disposed of in accordance with the Human Rights Act, Data Protection Act and in line with CPIA.
- 11.1.2 All media at the conclusion of its appropriate evidential lifecycle must be considered for recycling / destruction. VHS tapes must be degaussed and disposed of as confidential waste. CD/DVD's must be shredded and disposed of in accordance with existing force policy. Reuseable Media (USB/HDD) to be clear, purge or destroyed as per policy.
- 11.1.3 Further advice can be obtained from:

[Physical and Digital Evidence Retention Model and Review](#)
[Criminal Procedure and Investigations Act 1996 \(section 23\(1\)\) Code of Practice](#)
[004-2024-npcc-cctv-portfolio-webinar-october-2023_redacted.pdf](#)

12. Human Rights Legislation

- 12.1.1 Merseyside Police must act in a way that is compatible with the European Convention of Human Rights (ECHR). Of particular relevance to retention periods of CCTV is article 8 ECHR, which protects the right of an individual's private and family life.
- 12.1.2 Further advice can be found using the link shown below.

[ECHR Home](#)

13. Data Protection Act 1998

- 13.1.1 The Data Protection Act 1998 (DPA) will be relevant to the retention of CCTV if the footage held is about a living person who can be identified from that data.

[Data Protection Act 1998](#)

14. VEU - Security Policy

- 14.1.1 All staff engaged in the processing of CCTV and digital evidence must ensure that they comply with the 'Acceptable Use of IT' Policy.

[ICT Acceptable Use Policy & Procedure](#)

15. Protection of Freedoms 2012 (CCTV Codes of Practice: Aug 2013)

- 15.1.1 On the 12th of August 2013, the Surveillance Camera Codes of Practice came into force. The Codes are pursuant to Sec 29 of the Protection of Freedoms Act 2012. Merseyside Police is a 'relevant authority' as defined by Section 33 of the 2012 Act, and as such must show due regard to the code when exercising any function to which it relates.
- 15.1.2 Whilst this is a Code of Practice, it is pursuant to Sec 29 of the Protection of Freedoms Act 2012 and is admissible in evidence in criminal or civil proceedings and a court or tribunal may take into account a failure by a relevant authority to have regard to the code in determining a question in any such proceedings.
- 15.1.3 For further information [Protection of Freedoms Act 2012](#)

16. Digital Image Database

- 16.1.1 The DID is the system for circulating images of unknown suspects and has been introduced to ensure that we are complying with PACE Code D. PACE Code D governs the exercise by police of statutory powers to identify persons.
- 16.1.2 This supersedes force crime news, and any other local methods used to circulate images of unknown offenders.
- 16.1.3 The DID has several user-friendly features designed to simplify the process of identifying unknown suspects and improve positive outcomes. These features include:
- Intelligence identification which allows officers and staff to proceed with an identification if they recognise a suspect but have not met them in person.
 - MG11 auto-generation that links to the relevant Niche Occurrence
 - Automatic notifications for OICs to ensure positive identifications are not missed.

16.2 How to Access the DID

- 16.2.1 To access the Digital Image Database, you will need to use a force computer and when logged in, opening the Corvus application. Here you will be able to open the Digital Image Database (DID). The first screen you will see is a disclaimer and warning regarding the viewing and identification conditions you must agree to. Once you click "Agree and Continue", the next screen will be the main DID menu.
- 16.2.2 You will see a number of tabs along the top of the screen and also images of nominals currently on the DID. Any images that have been requested/agree to be displayed as high, will show at the top of the list. These images will have a red box around to highlight they are high nominals. All normal submissions will display below the high circulations and will be in date order.

16.2.3 Images are set to stay on the DID for one month and will be removed after this date. The requesting officer can request for this to be added the following month should there be no identification or at a later date.

16.3 Request Still to be added

16.3.1 To request a still to be added to the DID you need to do the following.

- The request is made via Niche. Using the Niche reference of the incident, the nominal image should be added to the report tab. The image should be from the original footage and the footage MUST not be secondary captured (photo from a screen). If the image is from secondary capture, then this will be rejected, and a request will be made for the requester to obtain a correct image. If the only image is secondary capture and there is no other way of obtaining the correct format, please update the OEL with this and the reason, this will then be considered by the Visual Intelligence Coordinator.
- If the image contains more than one person, then the other person(s) must be removed, this can be done by cropping the image to keep the nominal in screen (be careful not to adjust the image ration which will alter how they look) or by adding a black box over the other person(s). Once this is complete, this image needs to be exhibited by the officer e.g. DJ/01,
- If there are multiple images of the same suspect then each still needs to be exhibited and using a letter after each still e.g. DJ/01a, DJ/01b etc.
- If there are multiple suspects from the same occurrence, then different exhibit references need to be given to assist with creating the different suspects on the DID e.g. DJ/01 – Suspect 1, DJ/02 – Suspect 2 etc.
- A request can be made to add a short clip of the suspect to the DID. This can be done by adding the clip to NICE and creating a short (ideally 5 second) variant on NICE. This will need to be given an exhibit reference. Should the clip contain other people, then please submit a CCTV request to the *VEU, requesting the clip be redacted and clearly explaining which person(s) need redacting/blurring. This should be done before a DID request. Once this has been done, then submit a request for the clip to be added to the DID.
- Once the image/clip is available, then a request to have this added to the DID should be requested. This can be done by opening the OEL from the requested Niche reference. Click on new template and using a CCTV 2 template – Processing request, please fill in requested tabs. The tabs that need completing are as follows:
 - Exhibit Ref – Please put Exhibit reference and any description - Exhibit AB/1 – Image of unknown suspect 1 on reports tab.
 - Has exhibited disc been viewed to confirm evidential value – Yes.
 - Please indicate work – Still image for DID.

- 16.3.2 If the above three tabs are not filled in, then the request will be returned to requester to be completed. Should this request be High priority, please state this and give a reason why.
- 16.3.3 Once all details are added to the OEL, a task to *Visual Evidence Unit should be submitted. This will be reviewed by the Visual Intelligence Coordinator, and if all details are correct, this will be added to the DID. The “VIC” will update the OEL to confirm this has been added to the DID.
- 16.3.4 During the course of the investigation should the unknown suspect become known, then they MUST inform the VEU to request this circulation be removed.

16.4 How to view suspects on the DID

- 16.4.1 To view the Digital Image Database, open via Corvus. Once in the Digital Image Database you can either just scroll down the images and view all current images in the DID or you can use the tabs along the top to filter which images are shown. You may just wish to view all Wirral images for instance.
- 16.4.2 On viewing the images, you should select each image individually, this will give a better larger image of the suspect to view, but once viewed the suspect will now be “greyed out” which will make it easier for you to see which suspects you have viewed. Should you be able to identify one of the persons, you can now produce an identification statement. To complete this, all you will need to do is click on the person you recognise, this will now give an option to make an identification. Once you click this option, you will need to enter the answers to the prepopulated questions. Once this is completed, an identification statement will be produced and added to the Niche file. The circulation will be removed from the DID and the OIC and VIC will be notified of this identification.

16.5 Facial Recognition

- 16.5.1 Merseyside Police currently has access to two facial recognition programmes.

- PND RFR
- Motorola Comparison Manager Pro

- 16.5.2 There are two methods for the use of RFR capabilities.

- 1) FIB VEU responsibility.

The Visual Intelligence Coordinator will review all images when reviewing stills requests for the Digital Image Database. The VIC will triage all images and those that are suitable will be searched against a database of images held on Motorola Comparison Pro and PND RFR.

The VIC will update the OEL with an update to confirm that the image has been run through facial recognition software and will confirm if No identification has been made or if a match has been made. Should a match be made, the VIC will update

with a name that has been given, if PND or RFR (or both), if PND a percentage will be given. The VIC will also send a task to the OIC with this update. It will be the responsibility of the OIC to research this information provided to see if assists with their investigation. Facial recognition is intelligence only.

- 2) OIC request – not suitable for DID/covert/external forces.
- 3) PND user upon request