



Capture and Handling of Evidential Imagery Using a Digital Device Policy (Surrey and Sussex) (587/2025)

Abstract

This policy describes the circumstances when police officers and police staff may use Digital Equipment and how the integrity of all still images recorded is maintained, both during and at the conclusion of a police investigation.

Policy

1. Introduction

1.1 Digital imaging and associated computer technology is a rapidly developing environment which has enormous benefit for the swift and accurate outcome of investigations as well as being useful for publicity for both Forces. This policy is required to ensure police officers and police staff who capture and handle digital images using Force, or their own digital cameras or other imaging equipment do so in accordance with the procedures associated with this policy whilst complying with relevant legislation.

1.2 This policy

- Complies with the [Defence Science and Technology Laboratory \(Dstl\) Digital Imaging and Multimedia Procedure 2020](#) and Government Security Classification (GSC) section within [APP Information Management](#).
- Should be adhered to by all police officers and police staff undertaking imaging tasks for evidential purposes (see exceptions Section 2.2).

2. Scope

2.1 The associated procedures detail the circumstances when Digital Images should be captured and managed using Force digital devices in Surrey and Sussex. It also covers the use and management of personal imaging devices (mobile - smart phone / digital camera / tablet etc.) in the event that Force equipment is unavailable.

It should be noted that Surrey Police and Sussex Police Information Security Policy (722) and associated Remote and Home Working Procedure state that any removable media should be encrypted to prevent the loss or compromise of information.

This document relates to best practice however, it is accepted that for certain operation reasons local documented procedures may apply.

2.2 This document DOES NOT relate to images captured on Body Worn Video (BWV), which is subject to a separate Force policy. It also does not apply to the Forensic

Collision Investigation and Reconstruction Unit (FCIRU) and Crime Scene Services (CSS) as they have separate working practices that comply with departmental Standard Operating Procedures and the requirements of Quality Standards and the [Forensic science activities: statutory code of practice - version 2 - GOV.UK](#)

In addition, consideration should be given to the provenance of any images stored within NICHE, Pronto or NICE Investigate and where the 'master' image is defined and located.

3. Policy Statement

3.1 Surrey Police and Sussex Police will ensure that the use of digital cameras and other imaging devices (such as mobile data terminals, mobile / smart phones etc) will be in accordance with relevant guidelines and legislation to safeguard the integrity of any images taken. For criminal cases this will safeguard images and ensure they are 'fit for purpose' and able to stand close scrutiny in a court of law particularly with regard to authenticity and continuity. Failure to comply with this policy and procedure may result in a legal challenge of evidence at Court.

3.2 Reference material and documentation

The content, guidance and principles of the following documents should be adhered to:-

[DSTL Digital Imaging and Multimedia Procedure v3.0](#)

[Forensic science activities: statutory code of practice - version 2 - GOV.UK](#)

The Code of Practice (version 1.0) became statutory at 00:01 on 2nd October 2023. The current Version (v2.0) was published 2nd October 2025.

NPCC Police and CPS Digital Evidence Sharing_MOU_21112023.docx

For additional information and guidance see the Handling of Digital Media (Images, CCTV, Video and Audio) Policy (Surrey and Sussex) (610)

Procedure

1. Legal Boundaries

1.1 Digital imaging has become firmly established in the mainstream of public life and as a key enabling technology for the police service with enormous benefits for the swift and accurate outcome of investigations, particularly given the increasing use of network technologies.

1.2 Under [Article 8 of the Human Rights Act 1998](#), every person has the right to respect for their private and family life. In respect of minor assaults, no images will be taken unless with the consent of the victim in line with APP guidance regarding Photographic / Image evidence, Victim care issues or in the case of a person under 17 years of age requiring an appropriate adult to be present. In addition consideration should be given to [Fraser Guidelines and the Gillick competency test](#) (for young persons to provide informed

consent) as to whether the child has the maturity to make their own decisions and to understand the implications of those decisions may need to be applied to determine children's rights and wishes.

1.3 Under the [Regulation of Investigatory Powers Act \(RIPA\) 2000](#), authorisations must be obtained before some images are taken. Authority to capture images is implied where there is a requirement for the camera operator to record photographically any such evidence in digital format that will assist in an investigation. For examples on the type of images that can be taken, please refer to section 2 below. RIPA Regulations MUST be considered and applied for ALL covert activities.

1.4 The [Criminal Procedures and Investigations Act \(CPIA\) 1996](#) sets out our duty to retain, reveal and record evidential material. It is therefore necessary for an audit trail to be established when digital images are taken.

2. Occasions and Offences when Images may be Taken

2.1 At present the cameras can be used to take images for the following offences including, but not restricted to:-

(a) Minor Assaults - i.e. an assault that results in:-

- Scratch / Graze.
- Abrasion.
- Minor bruise.
- Swelling.
- Reddening of skin.
- Superficial cut.
- Black eye, etc.

(b) Criminal damage to property and vehicles.

(c) Disturbances at domestic incidents and burglaries which would show the scene before the clearing up process.

(d) Road Traffic Collisions (RTCs).

(e) Recovered stolen property.

(f) Shoplifting cases where the items stolen are perishable.

(g) Where a suspect is seen committing an offence, as long as the images are taken overtly i.e., not taken while hiding behind a wall or inside a building etc.

(h) Approved and authorised operational images such as seized alcohol, tobacco, graffiti tags etc.

(i) Sex offender for registration purposes.

(j) Offenders who are required to report to police stations whilst on police bail.

(k) Untimely deaths.

(l) For surveillance purposes (see section 1.3).

(m) During the execution of warrants.

(n) For other investigative purposes.

2.2 Victims of violence should be asked for their consent before any images are taken, and their wishes are paramount. Where clothing has to be removed to reveal injuries, consideration must be given to the individual and their gender (and possibility of having undergone reassignment surgery), sexual orientation, religion, faith, age or disability and their personal preference for who would be most appropriate to take the image. Where appropriate ensure the victim is accompanied by a chaperone or appropriate adult. Discretion should be used as to what area will be exposed and whether the victim is comfortable for the images to be taken. Images of intimate parts of the body will not be taken.

Where appropriate a scale (such as a ruler) should be used to demonstrate the size of the injury. In these instances, one image should be captured with a scale visible and another image without the scale.

2.3 Images of injuries of children can be taken by police officers and police staff. However, Crime Scene Services (CSS) - Senior Crime Scene Investigator (SCSI) or Crime Scene Investigator (CSI) advice MUST be sought if there are bite mark injuries or injuries sustained with an implement / weapon where there may be potential for subsequent dental or mechanical comparison. Senior CSIs can be contacted via e-mail.

2.4 Specialist ultraviolet (UV) light and cross-polarisation photography can be carried out by Crime Scene Services. These techniques have the potential to enhance and / or disclose current and historical bite mark injuries or injuries sustained with an implement / weapon that may no longer be visible to the naked eye.

Historical is determined to be at least six weeks old and will require photographing repeatedly throughout the healing process. All instances where this technique is considered should initially be discussed with a Senior CSI.

2.5 If the injuries are more serious than a minor assault, then the images must be captured by a CSI.

2.6 Any injuries received or alleged to have been received by a police officer, or member of police staff, in the execution of their duty will also need to be taken by a CSI unless

there is an immediacy for the images to be taken at the time and there are no CSIs available.

2.7 Surveillance images can only be captured with the correct RIPA authority.

3. Guidance on the Use of Police Cameras & Imaging Devices

3.1 Individuals must be conversant in the use of the camera equipment / device using the instruction manual where available.

3.2 The operator must check the time and date has been set correctly and ensure there is adequate battery life for the current task. Therefore, individuals should, where possible, ensure spare batteries are available.

3.3 The camera / device should be checked prior to use on each occasion to ensure the equipment is working correctly and should be returned in working order. Faults and/or damage should be reported to a line manager and faulty / damaged equipment taken out of service.

3.4 Individuals must ensure cameras / devices are kept secure when leaving vehicles unattended.

3.5 In order to ensure integrity of all images, any images taken at an incident **MUST NOT BE DELETED** even though the image may be out of focus or taken accidentally. The whole sequence of images must be kept. If any images are accidentally deleted before uploading, this must be recorded including a brief description of the subject matter. Images will only be deleted on a camera by formatting the memory card using the inbuilt menu of the camera's operating system, **AFTER** uploading the images onto NICE Investigate.

3.6 Individuals must make an entry in their pocket notebook or Mobile Data Terminal (MDT) of the number of images taken and that consent was requested and given. The number of images taken should not be more than is necessary to record a true picture of the incident. In addition, a record must be kept of the specific device used (including make, model and any unique reference or serial number).

3.7 Once the sequence of images has been taken, the images must be uploaded onto NICE Investigate as soon as practicable and, in any event, before the end of the individual's tour of duty or shift.

3.8 Once the images have been uploaded onto NICE the media card must be **formatted** using the camera's own menu to perform the function which will permanently delete all the data on the media card. This will prevent any corruption of new images against those already taken.

3.9 Best practice is to upload as soon as possible to reduce the time and opportunity for accidental, intentional, or malicious alteration of images. The integrity of images needs to be protected at the earliest stage as this reduces the opportunities for challenges at court.

3.10 The memory card in each camera must remain with that camera. It must not be transferred, as the captured media may not function correctly.

3.11 Due to exigencies of duty, it may be that police officers and police staff will have to take images of more than one incident before they are able to upload them onto NICE Investigate. This is not considered best practice however, if this occurs then they must, after each incident, make an entry in their pocket notebook of the incident attended and number of images taken so that each incident can be identified separately.

3.12 Alternatively, if there are additional memory cards available kept with the camera, then these can be used to record the separate incidents.

3.13 Only the Forensic Digital Media Unit (FDMU) has software installed on computers and the expertise to carry out 'enhancement' of images. If any image is submitted which is identified as having been previously manipulated, altered or is suspected to be, or is identified as a Deepfake / Synthetic Media it will not be accepted by the FDMU under any circumstances. The Chief Superintendent for the individual's Division will be notified and then be responsible for ascertaining how and why the image came to be altered or produced.

3.14 Any images that may be required for use in interview or for Charged and Bailed to Court Files should be uploaded to NICE Investigate and where absolutely necessary be printed locally on Force networked printers.

4. Use of Force Issued Mobile Data Terminals (MDT) or other Force Smartphones as an Imaging Device

4.1 All Force issue smart phone devices can take high resolution digital imagery either through the camera app on the device or via third-party applications.

4.2 When images are captured using the mobile policing application Pronto or directly via the camera app, a copy of the photo(s) are stored in the device's image gallery. Where these images are required for evidential purposes, it is the responsibility of the officer or staff member to ensure that these photos are uploaded to the Forces' evidential media platform NICE Investigate and attached to the relevant case file. Once the images are confirmed to be attached the relevant case file, the officer or staff member should delete the images from the devices image gallery.

5. Use of Personal Camera / other Equipment as an Imaging Device

5.1 It is recognised that at certain times a Force digital camera is not available to capture images of a crime. A new procedure has been developed which allows the use of personal devices in these circumstances which will ensure the requirements of the [UK General Data Protection Regulation \(UK GDPR\)](#), [Data Protection Act 2018](#) and [Freedom of Information Act 2000](#) are met and that the integrity of Surrey Police and Sussex Police's information infrastructure is not compromised. The Use of Personal Devices Procedure provides guidance - see the Surrey Police and Sussex Police Information Security Policy (722) for details.

5.2 When a personal device (meeting the criteria detailed in the use of Use of Personal Devices Procedure) is used to capture images, the operator **MUST** ensure the date and time are properly set for the UK (check with the Force computer clock).

5.3 BEST PRACTICE IS TO MASTER / UPLOAD IMAGES ON TO NICE Investigate AND NOT TO COPY ON TO A CD or DVD - although it may in some instances be necessary to do so for instance if NICE Investigate is not available or due to the highly sensitive nature of the images (see section 8.1).

Responsibility for uploading images to NICE Investigate sits with the creator or recipient of the images.

5.4 Police officers must realise that images taken may be scrutinised closely and challenges over their integrity may occur in Court. It is suggested a statement is written as to what camera or device (including make, model and any unique reference or serial number) the images were taken on and the subsequent audit trail. In this way, the police officer is complying with full disclosure and the decision to use the images for court purposes can be made at an early stage.

5.5 Surrey Police and Sussex Police will not be held liable for costs incurred for transmitting images / data or if damage is caused to personal imaging devices used in connection with an investigation whilst on duty. It is left to the individual's discretion as to whether they use their personal equipment.

6. Surrey and Sussex Forensic Digital Media Unit (FDMU)

6.1 Forensic Investigations have created a series of short videos to showcase what each department does. These include an overview of Crime Scene Services (CSS), the Forensic Recovery Unit (FRU), the Forensic Digital Media Unit (FDMU), the Forensic Identification Services Unit (FISU) and the Forensic Hub and what services they offer.

6.2 It is stressed that **ALL** images **MUST** be deleted from **ALL** devices once the images have been Mastered. Images **MUST NOT** be distributed elsewhere in the organisation or to external agencies, other than the Crown Prosecution Service (CPS) without the consent of your supervisor. **Be mindful of the breach of the Data Protection Act if images are taken home and displayed outside the organisation.**

7. Images Taken by Victims of Crime, Witnesses or Members of the Public

7.1 On occasions victims of crime, witnesses, or Members of the Public take, or are requested to take images of the crime e.g., Criminal Damage or injuries. In these circumstances the images should be forwarded to the Officer in the Case (OIC) via the NICE Investigate portal by way of a 'Citizen Request' (see Crib Sheet 17 in the Training area for NICE).

8. Digital Image Mastering Process

8.1 BEST PRACTICE IS TO MASTER IMAGES ON TO NICE Investigate AND NOT ON TO DVD although it may in some instances be necessary to do so - for instance, if NICE

Investigate is not available or due to the highly sensitive nature of the images captured. In these instances, both a Master and a Working copy Disc MUST be produced.

Regarding sensitive images / video that cannot be stored on or shared via NICE Investigate, the jointly agreed MoU states the following: -

- Indecent Images of Children - CPS should not receive this material in any format. Images should be described in a schedule and categorised. If these need to be viewed, then arrangements should be made to view them on a police device.
- Sexually Explicit and Graphic Images - This material can be held on Case Management System (CMS) and can be sent by police in a photobook URL. However, this material cannot be put onto DCS (Crown Court Digital Case System), as HMCTS (His Majesty's Court and Tribunal Service) have made clear that sexually explicit images (nudity/legal pornographic) and Graphic images should not be uploaded. This is because the DCS has a wider audience than CMS. To be served / disclosure via Secure Email (not via CC DCS). Prefix file name with 'Explicit Image' or Prefix file name with 'Graphic Image'

9. Downloading Images onto Hard Drives

9.1 As part of the investigation process, it will be permissible for images to be downloaded onto a hard drive and e-mailed to named police officers or members of police staff in an investigative role. This procedure is for investigative purposes only and must be correctly audited. At no time are officers or members of staff permitted to store these images in their personal account.

9.2 The images must first be uploaded onto NICE Investigate as detailed in paragraph 3.7 above. The working copy should then be placed into a Force network police computer only. Once the images have uploaded onto the computer, they should be sent via e-mail to the named police officer or member of police staff in an investigative role. Once the officer has confirmation that the images have been received and are viewable, they must then be deleted from the computer. The police officer or member of police staff must make a record of this process in their pocket notebook or MDT.

9.3 Once the images have served their purpose i.e., identification, printed for interview or charging decision, then these images must be deleted from the computer immediately. This should be recorded in case of a later challenge.

9.4 In addition to the above process, where images are taken before stolen property is returned to its owner, it is also permissible to download images onto the hard drive and upload them onto a property database. Once this has been completed the images should be deleted from the hard drive.

10. Downloading / Uploading Images - Sex Offenders Register

10.1 Under [Section 87 of the Sexual Offences Act 2003](#) it is permissible to take a photograph of a person for the purposes of verifying the identity of the relevant offender, which forms part of the 'Sex Offenders Register'. Under these circumstances it will be permissible for Public Protection Officers to upload these images onto a hard drive.

These can then be uploaded to the Registered Sex Offenders file within SharePoint and also onto the Violent and Sexual Offenders Register (ViSOR).

10.2 Once the images have been uploaded successfully, they **MUST BE DELETED** from the camera / device.

10.3 Indecent images of children must not be placed onto NICE Investigate under any circumstances. Such images should be considered for redaction which could then be uploaded to NICE Investigate. If redaction is considered it should be discussed with, and submitted to the Forensic Digital Media Unit (FDMU) who can conduct this work.

11. Audit Trail for Users

11.1 One of the fundamental requirements of digital imaging is the need to safeguard the integrity of images and part of this process involves an audit trail being started at the earliest stage. The audit trail must be recorded in the individual's statement and should follow a logical sequence as below:

- (a) Details of the case attended.
- (b) Description and number of images taken.
- (c) Creation of Master and Working Copy on NICE Investigate.

11.2 It is best practice for the person taking the images to also upload them. If, due to demands of duty, they are unable to complete this, their statement must include who carried out this task on their behalf. This person must also complete a statement as to the time, date and circumstances of their involvement.

12. Copyright and Applying the Government Security Classification Scheme (GSC)

12.1 Images generated by either Force and released outside of the Forces will be clearly copyrighted to relevant Chief Constable - Surrey Police or Sussex Police should be used when exporting images.

12.2 The principles of the GSC will be applied to all images generated by Surrey Police, Sussex Police, and third-party images at the point of transfer / receipt into Force. Force computer network system will only facilitate material classified up to 'OFFICIAL SENSITIVE' Therefore any images that are deemed to be above this classification will NOT be uploaded and will require handling as per the requirements of the GSC scheme.

12.3 Any request for an image(s) taken by police officers or police staff for media release must be passed to the relevant Media Relations Department.

13. Upkeep of Equipment

13.1 It will be the responsibility of Divisions to keep records of the make, model, serial numbers, and location of the imaging devices on their Division.

13.2 The Divisions will also be responsible for the upkeep of the cameras / imaging equipment including the cost of any repairs or damage to equipment.

13.3 Any new equipment must be purchased Divisionally or Departmentally via the Procurement process.

14. Retention Periods

14.1 Surrey Police and Sussex Police will retain their crime and Intelligence records in compliance with the minimum standards set by the Management of Police information (MoPI) and CPIA.

Crimes are no longer categorised as detected / undetected and everything stored on NICHE is assigned a MoPI grading.

Reference should be made to Surrey and Sussex Retention Schedule, and Information Management Policy (Surrey and Sussex) (1187) or by emailing Information Management.

Team: Specialist Crime Command Forensic Investigations