

WILTSHIRE POLICE



XXXX – Via email



Police Headquarters
London Road
DEVIZES
Wiltshire
SN10 2DN
disclosure@wiltshire.police.uk

Date: 10th July 2025

Our ref: FOI 2025-463

Reply contact name:

Dear XXXX,

I write in connection with your request for information dated 6th May 2025 regarding the extraction of digital data from victims of rape and serious sexual offences (RASSO).

I am required by the Freedom of Information Act 2000 to handle all requests in a manner that is blind as to the identity and motives of the requestor. Any information released as a response to a request is regarded as being published and therefore in the public domain without caveat.

Following receipt of your request, research was conducted, and I am able to respond as follows.

You wrote (and our response):

I have considered your request, and I am able to provide a partial response to your request. Some of the information relevant to this request is exempt by virtue of Section 31(1)(a) - Law Enforcement.

Section 31 is a qualified prejudice-based exemption and therefore requires Wiltshire Police to establish the harm in disclosure, along with the public interest favouring and against disclosure.

Specifically, we request disclosure of the following information:

1. Policies and guidance

a. Please provide copies of any current internal policies, procedures, guidance documents, or internal forms used by your force in relation to the extraction of digital data from victims or witnesses in RASSO investigations.

Under the Freedom of Information Act 2000 (FOIA), this question is partially exempt by virtue of Section 31(1)(a) - Law Enforcement. Please see the harm and balance tests below.

I have provided the R.A.S.S.O (Rape And Serious Sexual Offences) Policy – attached below – and under our Section 16 obligation to provide advice and assistance, I can confirm that we follow guidance produced by Op Soteria.

Keeping Wiltshire Safe

b. Please provide copies of any standard forms, information packs, or other materials provided to victims or witnesses when requesting access to their mobile phones or proposing a download of their data.

Please see the document attached below.

2. Compliance with new legal framework

a. Has your force adopted the new Code of Practice issued under section 37 of the Police, Crime, Sentencing and Courts Act 2022? If so, please provide the date of adoption and any associated implementation documents.

No – We already had processes in place that reflect those that are set out in the code of practice.

b. Has your force issued any training or operational guidance to officers on the use of the Code and the new statutory framework? If so, please provide details (including training materials if available).

N/A – We use the Op Soteria NOM.

(<https://www.wiltshire.police.uk/news/wiltshire/news/2023/july-2023/operation-soteria/>)

3. Technology and digital extraction tools

a. What tools or software systems are currently used by your force to extract digital data from mobile phones in the context of RASSO investigations? Are these tools used consistently across all RASSO cases?

Odyssey.

No – Odyssey is only for adult rape and attempt rapes, and you will be seeking something different when investigating child offences.

b. Are these tools configured to allow selective extraction (i.e. only of relevant material), or are they routinely used for full downloads?

Yes – Odyssey enables us to make a selective extraction.

c. Has your force conducted any audits or reviews of the use of digital extraction tools since the introduction of the new legislation and Code of Practice?

No. Odyssey is overseen and implemented by Southwest Forensics.

4. Oversight and accountability

a. Does your force have a panel or mechanism for reviewing RASSO cases where a victim or witness has challenged a request for access to their digital data? If so, does that panel or mechanism remain in place?

No – It is so rare as Odyssey ensures this doesn't happen and we are so careful with what we request

b. Does your force collect internal data on how many times digital data has been extracted from victims or witnesses in RASSO cases in the past two calendar years? If yes, please provide those figures.

No

c. Has your force received any complaints about mobile phone data extraction practices from victims or witnesses in RASSO investigations during the last two years? If so, please provide the number of such complaints.

No

Harm test

Disclosing information into the public domain – specifically internal documents in relation to the extraction of data from victims and witnesses – would undermine the core principles of policing; namely to prevent and detect crime. Disclosure of this information could cause substantial harm to planned policing operations, and all individuals involved i.e. police employees and the community. If Wiltshire Police were to place this information into

Keeping Wiltshire Safe

the public domain, this would prejudice our ability to prevent and detect crime, and to apprehend or prosecute offenders; providing offenders with the information they would need to evade detection and therefore effecting the Force's ability to protect the community.

Factors favouring disclosure

Placing this information into the public domain would lead to an increased public awareness of these issues. This in turn may lead to a reduction in crime or more information being supplied by the public and would also allow the public to better protect themselves against crime. Disclosure would also ensure that Wiltshire Police can be held accountable for the actions taken, and show the Force as being as open and transparent with the public as possible.

Factors against disclosure

Disclosing internal documents and guidance in relation to the extraction of digital data from victims or witnesses in RASSO investigations into the public domain would hinder the prevention and detection of crime. This would result in investigations being compromised, as offenders would be able to gain valuable information that would assist them in evading prosecution. By offenders evading prosecution, the public will be put at a greater risk, resulting in trust in the Force diminishing and increase of crime being seen. Disclosure of information sensitive to operations and tactics used would severely impact on the Force's resources, also assisting offenders to evade capture.

Balance test

Whilst there is a public interest in transparency and openness between the Force and the public, in addition to the public seeing how the Force are engaging with the threat from criminals, there is a stronger interest in ensuring the public are protected from the threat of criminals, and that the enforcement of the law and the prevention and detection of crime is upheld. To disclose information which is likely to assist offenders would seriously undermine the effective delivery of operational law enforcement and is therefore exempt from disclosure.

Section 17 of the Freedom of Information Act 2000 requires the Constabulary, when refusing to provide information (because the information is exempt) to provide you the applicant with a notice which: (a) states that fact, (b) specifies the exemption in question and (c) states (if that would not otherwise be apparent) why the exemption applies.

In accordance with the Freedom of Information Act 2000 this letter acts as a Refusal Notice for those aspects of your request.

Exemptions applied:

Section 31(1)(a) - Law Enforcement

I am satisfied that all the relevant information has been passed to me and considered in the light of your request within the time constraints applicable under the legislation.

Wiltshire Police would like to thank you for the interest that you have shown in the Force.

Yours sincerely

Force Disclosure Decision Maker
Keeping Wiltshire Safe



R.A.S.S.O. (Rape And Serious Sexual Offences) Policy

^ Table of Contents.

[POLICY STATEMENT.](#)

[STRATEGIC INTENT.](#)

[APPLICABILITY.](#)

[POLICY AIMS.](#)

[Terminology.](#)

[Victim or Survivor's Gender.](#)

[POLICY APPROACH TO RASSO INVESTIGATIONS.](#)

[THE FIRST RESPONSE TO RASSO.](#)

[Victim Safety & Wellbeing.](#)

[Early Evidence & Disclosure.](#)

[FORENSIC EVIDENCE.](#)

[Victim Body Swabs.](#)

[Toxicology.](#)

[Forensic Integrity.](#)

[Urgent Forensic Submissions.](#)

['Non Recent' Offences.](#)

[Consent.](#)

[VICTIM SUPPORT & SAFEGUARDING.](#)

[Sexual Assault Referral Centre \(SARC\).](#)

[Victim Self-Referral to SARC.](#)

[VICTIM SAFEGUARDING.](#)

[INVESTIGATIONS & CASE MANAGEMENT.](#)

[THE 24 HOUR COMMITMENT - Digital Evidence Retrieval From Victim Devices.](#)

[Interviews of Victims.](#)

[NCA SERIOUS CRIME ANALYSIS SECTION REFERRAL.](#)

[EARLY INVESTIGATIVE ADVICE \(EIA\).](#)

[SUPERVISORY OVERSIGHT.](#)

[Rape \(including attempts\) NFA Decisions \(Police\).](#)

[Delivering NFA Decisions.](#)

[RELATED DOCUMENTS and Authorised Professional Practice.](#)

[DATA PROTECTION AND FREEDOM OF INFORMATION.](#)

[HUMAN RIGHTS AND EQUALITY IMPACT.](#)

[REVISION HISTORY.](#)

POLICY STATEMENT.

Rape and serious sexual offences, known as 'RASSO', are among the most serious and high-impact crimes against the person. Wiltshire Police is committed to playing its role in partnership with the Home Office, the Crown Prosecution Service and local and national support services in identifying, targeting and bringing to justice perpetrators, and, supporting and increasing confidence of victims, survivors and effected communities.

To achieve this aim, this RASSO Policy will support colleagues and partner agencies in understanding the strategic intent of Wiltshire Police.

This policy acknowledges and supports the operating model developed by the national research and change program: Operation Soteria Bluestone, the National Violence Against Women and Girls (VAWG) Strategic Threat Assessment and the Authorised Professional Practice for Rape and Sexual Offences.

Wiltshire Police acknowledges that RASSO offending crosses a broad spectrum of other criminality (for example: domestic abuse, honour-based abuse (HBA), criminal exploitation, offences against children) and that offending can remain hidden and unreported due to victims' feelings of fear, misplaced shame or embarrassment, isolation from support or mistrust of police or the criminal justice system.

Public trust and confidence in policing have been eroded over recent years. A series of high-profile cases have impacted women and minoritised groups confidence in policing, particularly in relation to how policing responds to crimes disproportionately affecting women and girls.

An independent report, authored by the co-academic lead from the Soteria Bluestone programme, reinforced the findings from the government's End-to-End Rape Review, and highlighted that policing needs a capable and confident workforce which understands the nature of rape and sexual offences and utilises this knowledge to thoroughly investigate suspects and better support victims.

STRATEGIC INTENT.

Wiltshire Police will:

- Work to Build trust and confidence in the police service so that victims feel safe to seek our help directly.
- Encourage reporting of all forms of sexual offending and provide effective means of reporting intelligence.

- Ensure that RASSO offences are thoroughly investigated by appropriately skilled police personnel.
- Provide effective support to victims of RASSO crimes, recognising & responding effectively to risk, keeping victims safe and holding offenders to account.
- Signpost every victim of RASSO offences to appropriate support agencies.
- Ensure that victims or survivors personal details are stored, managed and handled with integrity and confidentiality
- Proactively engage with victims and survivors of RASSO crimes to obtain feedback on the effectiveness of the service.
- Engage with the Crown Prosecution Service and the Tri-Force Wessex RASSO governance structures to understand force and regional performance.
- Provide effective support to Wiltshire Police personnel tasked with responding to, and investigating, RASSO ensuring they are:
 - Properly trained according to national guidelines
 - Provided with effective support in relation to their emotional wellbeing and mental health

APPLICABILITY.

This policy applies to all police officers and staff, including volunteers, whether they are first responders, investigators, welfare or safety support, case managers or supervisors of personnel in these roles.

Any member of Wiltshire Police who may have contact with victims, witnesses and suspects of RASSO, their families or associated members of the community should be aware of this policy.

The policy applies equally to all RASSO offences, whether there is a standing relationship (regardless of the time scale of the relationship) between victim(s) and suspect(s) or not.

POLICY AIMS.

This document does not provide a RASSO investigative toolkit but will instead define RASSO and direct responders and investigators to local procedures and signpost to national learning, guidance and Authorised Professional Practice for the initial response and investigation (including victim care) of RASSO cases.

Terminology.

The term RASSO is used in relation to the following sections of The Sexual Offences Act 2014:

- Section 1: Rape
- Section 2: Sexual Assault by Penetration

ACPO Guidance for Investigating and Prosecuting Rape 2010 defines other serious sexual offences as:

- Where the assault is particularly serious
- Where features of the offence are aggravated (for example, where the victim is vulnerable or the offence is linked to Hate Crime).
- Sexual assaults that are linked as a series to the same offender(s).
- Any other offence of a sexual nature deemed especially serious by the investigating officer
- An attempt to commit any of the above offences

Where the victim of a serious sexual offence is under the age of 18, then this policy should be applied in conjunction with the [Child Abuse Procedure](#).

Police officers and staff should consider whether identified victims might be at risk of linked criminality or harmful practices, **particularly Domestic Abuse and Honour Based Abuse (HBA)**. In cases where such risk is reported, suspected or feared, officers and staff should take appropriate steps to identify particular risks, protective factors and sources of support.

Risk assessment and safeguarding is not simply the responsibility of a single point of contact or unit. Every member of Wiltshire Police who has contact with a RASSO victim should consider:

- the context of the investigation
- whether any new incident, event or information may affect the risk to the victim, and
- take appropriate action to ensure the risk is reduced or removed.

Victim or Survivor's Gender.

Clear evidence shows that females are statistically much more likely to be targeted by RASSO offenders, and RASSO offenders themselves are overwhelmingly male. However, Wiltshire Police acknowledges that RASSO can have a devastating affect regardless of the victim's gender. As such, the label 'victim' or 'survivor' in this policy applies equally to any person of any gender.

POLICY APPROACH TO RASSO INVESTIGATIONS.

In response to rape and serious sexual offences (RASSO) reports, all Wiltshire Police personnel will adhere to The Operation Soteria Bluestone national operating model approach, which is underpinned by three fundamental principles.

Wiltshire Police RASSO investigations must be:

Victim-centred:

Procedural justice principles underpin all officer and staff interactions with victims. Victim rights and needs inform officer decision-making in RASSO investigations.

Suspect-focused:

Specialist knowledge about sexual offending behaviour and its impact on victims informs RASSO investigations and offence prevention. Officers are bound to act consistently with the human rights of suspects and victims, as set out in the European Convention on Human Rights (ECHR) and incorporated into domestic law by the Human Rights Act 1998.

Context-led:

Officers take the context of the offence into consideration from the moment the offence is disclosed to police. This includes the:

- victim-suspect relationship context
- victim context, including whether they want an investigation
- suspect context, uncovered through a suspect-focused investigation

The meaning of 'Context' is to take into consideration the conditions that surround an event or situation, so giving it a fuller or more identifiable meaning than if simply dealt with in isolation.

The Investigator's Journey guidance is central to this model and shows how policing can use this approach throughout the investigation. This guidance can be found on the force's [Operation Soteria Bluestone Sharepoint](#) page.

THE FIRST RESPONSE TO RASSO.

The swift, effective response to, and thorough investigation of RASSO is critical. The current [Crime Screening and Allocation Procedure](#) states that generally, PIP 2 (Professionalising Investigations Programme, level 2) trained investigators from CID or CAIT will deal with penetrative sexual offences (including attempts and non-recent cases).

If there are aggravating factors in any other RASSO case which suggest it may be more suitable for PIP 2 investigation, this should be discussed with the relevant CID or CAIT supervisor.

It is important to acknowledge that during hours outside of normal CID or CAIT duties, initial response to a victim of a RASSO offence may fall to PIP1 trained 'uniformed response' personnel. In such circumstances the FIM should contact the Duty Detective Sergeant for advice.

Please see [SOIT On Call - Terms of Reference](#) and [TOR SOLO deployment from 090112](#).

Responders, investigators and safeguarders must be alert to the status of a victim of serious sexual offences as 'Intimidated' (under section 17 of the Youth Justice & Criminal Evidence Act 1999) and, as such, they will have 'Enhanced Rights' as set out in the [Code of Practice for Victims of Crime](#).

It will be beneficial for first responders to have read and understood the College of Policing [Briefing note for police first responders to a report of rape or sexual assault](#) which clearly states that the quality of your initial response may influence the victim's decision to support the investigation and in ALL cases you should:

- ensure the victim's safety, understanding any risk posed by the perpetrator to the victim or other people
- identify any immediate medical needs
- initiate the investigation and consider evidence preservation from the outset
- reassure the victim that they have done the right thing in coming forward and reporting
- be non-judgemental
- show empathy and sensitivity
- maintain impartiality
- identify if an interpreter or registered intermediary is required
- speak to the victim in an environment in which they are comfortable
- understand that rape and sexual offences in intimate or ex-intimate partner relationships may occur as part of a pattern of coercive or controlling behaviour or stalking and seek evidence connected with either of these offences
- remember that many victims may be under the age of 18 and are therefore still children and need to be dealt with in accordance with current Working Together to Safeguard Children guidance and Authorised Professional Practice on child abuse investigation.

If a body worn video device is deployed by a first responder, this must only be used to obtain an initial account and only where the victim consents and has the capacity to consent (see [Body Worn Video Procedure](#) section 2.5).

Victim Safety & Wellbeing.

On initial contact, the condition of the victim should be ascertained and if it is apparent that the victim is injured, or is in need of some other medical treatment, suitable arrangements should be made. The safety and wellbeing (both physical and mental) of the victim is the over-riding priority. Those with neuro-diverse or physical disabilities or conditions may need additional support to preserve their health.

Early Evidence & Disclosure.

In relation to deployment of resources, all Wiltshire Police personnel should note the guidance within [Authorised Professional Practice for the investigative process](#) ('First Investigative Steps'), which states:

'The first chance to obtain material may also be the last. The speed of investigative action and the deployment of resources to a scene will increase the chance of protecting, preserving or gathering material that may otherwise be contaminated or lost. It may also improve the chances of identifying and apprehending the suspect earlier.'

When attending as a first responder to a victim of RASSO it is vital that an officer has due regard for the Golden Hour 'Five Building Block Principles' (as defined in Section 1.4.2 of the [Major Crime Investigation Manual](#)):

1. Preservation of Life
2. Preserve Scenes
3. Secure Material
4. Identify Victims
5. Identify and Arrest Suspects

The officer must have with them as a minimum: an **Early Evidence Kit** and a **First Response Booklet: RASSO**. Both of these items should be kept in marked response vehicles.

An electronic version of the First Response booklet is available at the SharePoint Document Centre (Forms & Templates) page ([Form number 1073](#)).

An [Early Evidence Kit video guide](#) is available on the [RASSO Sharepoint](#) site's First Responder Toolkit page.

FORENSIC EVIDENCE.

RASSO cases may provide an opportunity to prove forensically that sexual and/or other physical contact has taken place. It is essential that in our initial response we identify forensic opportunities which may help support lines of enquiry. FFLM Sampling guidelines provide windows of forensic opportunity for physical samples (NOTE: these guidelines are reviewed and refreshed twice per year, so it is important that the latest version is obtained from the website. DO NOT keep and refer to old versions as the guidance in these may now be incorrect). In addition, investigators should be aware of physical injury and task CSI to record those injuries at the time and or in a succession of visits to record emerging injuries.

It is important for first responders to note that, even if a victim is booked to complete a forensic medical, it is best practice to complete an **Early Evidence Kit** prior to transport to Sexual Assault Referral Centre (SARC). Vital forensic evidence could be lost in the time it takes to get to the SARC, for example, the victim may need to urinate or take on fluids prior to the forensic medical commencing and there a risk (albeit small) of cross contamination when travelling in police vehicles.

It is also important to consider any other evidence that may be at scene, for example discarded tissues, condoms, clothing, drinks bottles, cigarette ends, body fluids, etc. Any potential evidence must be secured as soon as is practicable. Contact the duty DS and or a CSI Manager for further advice.

Victim Body Swabs.

Ideally, skin swabs should be taken from RASSO victims as part of a forensic medical. **Victims should only be asked to self swab in exceptional circumstances** (so, where the alternative is that the forensic evidence will be lost) bearing in mind the fact that they will not be doing this in a forensically clean environment.

Investigators must not swab intimate areas of a victim. Be aware that an 'intimate' sample referred to in relation to victims differs from a suspect intimate sample as defined by Section 65 of PACE 1984. Investigators must avoid taking any skin swabs from an area of a victim's body which would be ordinarily covered by underwear. In addition, investigators must exhibit caution when considering swabs near intimate areas (e.g., the inner thighs).

Investigators should always consider obtaining advice from SARC (in or out of normal hours) – this is particularly important considering the fact that the victim may need a high level of support that a crisis worker is best placed to provide. Though taking a first account and securing evidence is a vital part of the initial investigation of RASSO, police personnel must be mindful that a victim cognitive function could be impaired by the extreme trauma of their ordeal, have misplaced feelings of shame and embarrassment or be fearful of police and authority, which could leave them unable to initially disclose the full details of what happened. An appropriately trained member of SARC may be able to elicit a more accurate and detailed account from the victim and properly assess the victim's immediate medical and welfare needs.

Toxicology.

Where toxicology is to be requested, a detailed history of medication for a victim or suspects may be required. If in doubt, investigators should consult with a CSI.

Forensic Integrity.

It is vital that when any seized evidence that may have forensic value is immediately placed into a forensically clean container or bag and **sealed at the time of seizure**, prior to moving from the current location. A detailed description of the item must be recorded on the exhibit label along with details of continuity to aid identification and maintain the integrity of the exhibit.

Forensic items must **NOT** be later removed from packaging as doing so can cause damage to the integrity of the evidence and further examination by the laboratory could be refused. Further, evidence could later be undermined by the defence in relation to cross-contamination arguments. Therefore, forensic evidence must not be removed from its container unless done so in a forensically clean environment under the guidance of a CSI.

Urgent Forensic Submissions.

Where investigators consider urgent submissions to forensic providers, contact must be made with the On Duty Regional Forensic Coordinator (RFC), details of which are held by local CSI. The RFC will determine and authorise evidence for urgent submission. The RFC must be provided with details of the victim's first account, physical evidence and samples already obtained, together with **Early Evidence Kit** and FFLM documents.

'Non Recent' Offences.

Regardless of the passage of time, there may be forensic opportunities. On a case-by-case basis, investigators should consider conducting a forensic review with local CSI managers, of victim and suspect accounts together with a review of physical evidence.

Consent.

Where consent has the potential to be raised as a defence (e.g., victim and suspect are in a domestic relationship), the tasking of CSI should still be considered. CSI may attend scenes to both search for and record evidence or the location's environment to support reasonable lines of enquiry in accordance with our CPIA obligations.

VICTIM SUPPORT & SAFEGUARDING.

Sexual Assault Referral Centre (SARC).

Every adult victim of RASSO crimes **must** be signposted to the SARC. The investigator must explain their right to seek support, aware that SARC provides for much more than just the forensic medical.

Always consider the need for urgent medical and welfare advice and be aware that, if emergency medical care is not required at a hospital, SARC will be able to triage the case and if appropriate offer this service. Timescales may be crucial and victims should be advised, for example, that a maximum of 72 hours applies to start HIV treatment and emergency contraception needs to be taken within five days.

The need for medical treatment should be carefully considered regardless of the age of the victim. Although a child may not be considered for pregnancy screening, etc., longer term health and wellbeing must be considered. For example, if Chlamydia is left untreated it can damage a victim's reproductive system, causing permanent infertility.

Victim Self-Referral to SARC.

Where a victim is unable to support a police investigation and or is unable to consent to forensic medical examination, they must as soon as is practicable be informed of their right to self-refer to SARC and be offered contact details.

Every member of Wiltshire Police who has contact with a victim must bear this in mind and pass on the information if the victim is hesitant in voicing their support for police action.

It may be that the victim will require time to process their ordeal before they can engage with support. SARC staff may be able to proactively contact a victim who currently does not wish to engage with the service. Where a victim refuses referral they must be asked at an early opportunity whether they would consent for police to pass their details to SARC for contact to be made from that service at a later time. This decision and whether the victim consents or not, should be recorded.

Where a victim had previously self-referred then later reports to police, the investigator allocated to the case **must at the earliest opportunity** obtain written consent from the victim for police to take any forensic samples previously taken by SARC into police evidence. This signed consent must be provided to the SARC before they will release the forensic samples.

VICTIM SAFEGUARDING.

The safety and welfare of a victim of RASSO must be central to the police response. This is particularly important in cases where the offence occurs within a domestic setting, where the victim is particularly vulnerable due to one or more protected characteristics being a factor, where the suspect is in a position of trust, where honour-based abuse is present, or where the suspect has engaged in stalking behaviours.

In circumstances where a PPN should be submitted, this must still be done and safeguarding appropriate to the identified risk level completed by the initial responder (regardless of whether that responder is uniform or non-uniform police personnel).

Police personnel must be aware that **levels of risk can fluctuate, so safeguarding opportunities must be considered whenever there are changes in circumstances**. For example, risk can escalate if a victim or suspect becomes homeless or if a victim withdraws support for the investigation. A 'flash point' can occur when a significant point of progress in the case is reached - for example, when a suspect becomes aware of a report to police, at the point of arrest or any release from custody or at the point of charge or discontinuance (by police or CPS).

Further to the safety of the victim, all police personnel must consider the risk of further sexual violence a suspect could pose to other members of the public, outside of the current case. Conducting a suspect led investigation and completing extensive intelligence background checks can assist in this regard, as well as considering information and intelligence from the victim(s), witnesses and other third parties and professionals.

All investigators of RASSO offences are encouraged to use the [Suspect Check List](#) aide memoire, available on the Operation Soteria Bluestone SharePoint site.

Further information around safeguarding, risk assessment, information sharing and partnership working can be found in the following force guidance:

[Domestic Abuse Policy and Procedure](#)

[Honour Based Abuse \(HBV\) Policy](#)

[Honour Based Abuse FGM and FM Procedure](#)

[Stalking and Harassment Policy and Procedure](#)

[Child Abuse Procedure](#)

INVESTIGATIONS & CASE MANAGEMENT.

When building cases, investigators are encouraged to view the Force RASSO and Operation Soteria Bluestone SharePoint sites along with [CPS case building](#) guidance.

THE 24 HOUR COMMITMENT - Digital Evidence Retrieval From Victim Devices.

Officers and staff who investigate adult rape cases where digital media evidence may need to be obtained from devices belong to the victim must be aware of the requirements of The Home Office 24 Hour Commitment 2022.

In order to raise public confidence around the investigation of rape, the Home Office published 'The 24 hour commitment'. The commitment, which sits alongside Operation Soteria Bluestone, states that no adult rape victim should be without a phone for more than 24 hours during a rape investigation.

Where it is possible and timely to do so, an investigator must consider alternatives to removing an adult rape victim's device as this potentially will leave that person unable to access help and support (or at least make accessing help and support more difficult and so causing further potential distress to the victim).

Alternatives to taking possession of the device are:

- Digivan deployment

- Op Odyssey deployment

If there is no other alternative but to request consent from the victim to take possession of their device, appropriate safeguarding of the victim (including consideration of providing a temporary replacement device at the force's expense) must be considered and recorded. All efforts must be made to ensure the victim's own device is returned within 24 hours.

If a device is not returned to an **adult** rape (or attempted rape) victim within 24 hours, the appropriate form: [THE 24 HOUR COMMITMENT \(office.com\)](#), must be completed and submitted to DIU as soon as possible.

Interviews of Victims.

All interviews of victims of RASSO should be planned and conducted in accordance with the standards set out in [Achieving Best Evidence In Criminal Proceedings](#) (ABE) guidance.

If a victim chooses to forego parts of the ABE process, for example, 'opting out' of Video Recorded Interview (VRI), or does not wish to be considered for Special Measures, it is critical that these decisions are recorded.

Interviewers must also be aware that the victim has 'Enhanced Rights' set out in the [Code of Practice for Victims of Crime](#) and therefore has a 'right' under the code to request that the police officer conducting the interview is of a gender of their choice. The police must meet such a request unless doing so would prejudice the fairness of the proceedings. If the request is not met, the investigator must explain the reasons why to the victim and record the rationale appropriately.

NCA SERIOUS CRIME ANALYSIS SECTION REFERRAL.

The NCA Serious Crime Analysis Section (SCAS) works to identify the potential emergence of serial killers and serial rapists at the earliest stage of their offending. The SCAS database is a national dataset of over 33,000 serious sexual offences, including over 960 murders.

It is vital that, if the criteria is met, the case details are sent to SCAS within twenty days, whether the offence is detected or undetected.

The [Serious Crime Analysis Sharepoint](#) page provides details of the criteria for a submission, a process map and contact details for the Force SPoC.

EARLY INVESTIGATIVE ADVICE (EIA).

Early consultation is a requirement for rape cases under the Director's Guidance on Charging. It is therefore vital that in all rape cases that are capable of a criminal justice outcome, the OIC considers whether early advice should be sought from CPS Wessex RASSO. The 2020 CPS Wessex 'Partnership Working & Early Advice' newsletter gives the guidance to police and is available on [EIA Sharepoint page](#), along with other advice and guidance for RASSO investigators.

Consideration of early advice is particularly important in cases involving a witness under 10 years of age (see section 5 of the [Police/CPS/HMCTS Young Witness Protocol](#) guidance).

Although EIA should always be considered, it is **not mandatory for every rape case**. However, where a case does meet the criteria for referral but the OIC decides not to bring the case to CPS for early advice (e.g. the early advice will not add value to the investigation), the OIC or their supervisor should record a clear rationale explaining this decision.

SUPERVISORY OVERSIGHT.

It is critical that supervisors have robust oversight of RASSO cases to ensure they are suspect focused, victim centred, context-led and are progressed at an acceptable rate.

All supervisors must comply with force [Hierarchical Crime Review Procedure](#), and be aware of the procedure in relation to rape cases specifically (referred to in Section 6 of the procedure).

Rape (including attempts) NFA Decisions (Police).

Where an investigator provides a rationale that a case should be submitted for No Further Action (NFA) without submitting the file to CPS RASSO for a charging decision, the investigator's detective sergeant must notify a detective inspector (usually the DI responsible for the unit or team) to request authority to discontinue the case.

The DI must provide a written rationale as to why the case is appropriate for NFA and only then can the case file be submitted to crime auditors for closure.

Delivering NFA Decisions.

The Investigator's priority at the point of NFA must always be for the victim to be informed of the decision as soon as is practicable whilst remaining sensitive to the impact this could have on them.

Investigators must think carefully about how this message is to be delivered and consider whether a third party, such as ISVA, other support service or friend or family member nominated by the victim could assist in communicating the message and offer support.

NFA decisions must be delivered face to face unless there are circumstances preventing this occurring or the victim requests a different form of contact. Letter templates and other guidance is available in the [Operation Soteria Bluestone Sharepoint site](#).

RELATED DOCUMENTS and Authorised Professional Practice.

- [Authorised Professional Practice for Rape and Sexual Offences](#)
- [Code of Practice for Victims of Crime](#)
- [Domestic Abuse Policy and Procedure](#)
- [Crime Screening and Allocation Procedure](#)
- [Honour Based Abuse \(HBV\) Policy](#)
- [Honour Based Abuse FGM and FM Procedure](#)
- [Stalking and Harassment Policy and Procedure](#)
- [Child Abuse Procedure](#)
- [Hierarchical Crime Review Procedure](#)
- [SOIT On Call - Terms of Reference](#)
- [TOR SOLO deployment from 090112](#)

DATA PROTECTION AND FREEDOM OF INFORMATION.

Any information relating to an identified or identifiable living individual recorded as a consequence of this policy will be processed in accordance with the Data Protection Act 2018, General Data Protection Regulations and the Force [Data Protection Policy](#).

This document has been assessed as suitable for public release.

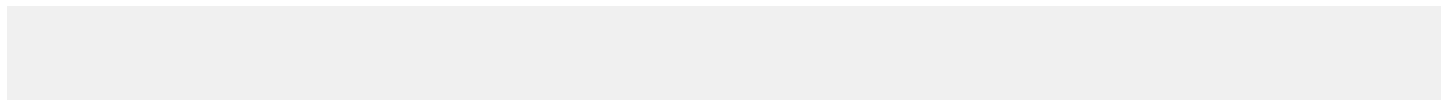
HUMAN RIGHTS AND EQUALITY IMPACT.

This policy has been drafted to comply with the principles of the Human Rights Act 1988 and Equality Act 2010. Members of Wiltshire Police administering this policy are responsible for ensuring that in its application, those to whom the policy applies, shall not receive less favourable treatment because of their age, colour, disability, ethnic or national origin, gender re-assignment, marital status, nationality, race, religion, sex or sexual orientation.

This policy has been subject to an equality impact assessment and has been graded High Impact. A full Equality Impact Assessment can be found on the [Equality Impact Assessment SharePoint page](#).

^ Revision History

Version	Date	Summary of Changes
1.0	15.12.2023	First publication.
1.0	11.03.2024	Slight amendments made re. FFLMS guidance and consent from victims for their details to be provided to SARC by police.



Security Classification/FoI 2000	Official – Yes under FoI
FoI Requests on rationale	npcc.foi.request@cru.pnn.police.uk
Author	ACC Jeremy Burton
Force/organisation	NPCC Disclosure
NPCC Coordination Committee	Criminal Justice
Telephone number	01483 633146
Date created	14/12/18



Obtaining data from digital devices during the course of an investigation

1. Executive Summary

In March 2018, Privacy International published a report entitled, “Digital Stop and Search”. This focussed on the extraction of data by police from electronic devices of witnesses, complainants and suspects during the course of a criminal investigation. This organisation claimed that police processes were flawed, describing “a potentially unlawful regime operating within UK police forces, who are confused about the legal basis for the technology they are using.”. It went on to say “The police are acting without clear safeguards for the public and no independent oversight to identify abuse and misuse of sensitive personal information”.

Whilst the content of the Privacy International publication is less than complimentary in terms of policing practices, it is generally pragmatic in its approach and recommendations. Consequently, it highlights risks for investigative practice in policing.

CC James Vaughan, NPCC Forensic Science, convened a gold group to respond specifically to this report, but the broader issue remains concerning the legality and consistency of approach by police forces when downloading digital data. Therefore, under the NPCC CJ Co-ordination Committee, a ‘Task and Finish’ working group was established consisting of colleagues from relevant areas (see table 1) to:

- Explore the legal framework available to investigators when seeking to download data from digital devices belonging to complainants and witnesses;
- Establish whether consent is required for such a download and how that consent should be obtained, recorded and managed through the course of the investigation;
- Recommend what information should be provided to a complainant or witness concerning how their data and third party material will be handled, stored and retained; and
- Propose a standard approach to be introduced nationally to ensure consistency.

Following the initial scoping exercise by the working group, instructions from counsel have now been received providing advice on the powers available for the search, seizure and examination of devices. In summary, there is no statutory provision to seize, examine and download data from witnesses or complainant’s digital devices. The only method by which we can take possession of digital devices from complainants and witnesses and download their data is through informed and ongoing consent.

Forces have hitherto developed their own methods of obtaining and recording such consent, but the inconsistency in approach is unhelpful. The focus of the Task and Finish group has therefore been to develop a national methodology for obtaining and recording informed consent at various points in an investigative process and with regard to a range of material, including that held by third parties.

There is risk in this approach since it is not currently supported by legislation but in the absence of an alternative, what has been developed is a practical solution for investigators and does address many of Privacy International’s concerns, especially in relation to clear and transparent information. The following recommendations are proposed:

1. The reliance on Sec. 19 PACE 1984 is to cease in these circumstances, as it is not an appropriate use of the legislation
2. All forces to provide complainants and witnesses information about why devices and 3rd party material may be required during the course of an investigation. (Appendix A).

3. Consent for 1) above is to be recorded on the appropriate document (Appendix B) and forces are advised to use this attachment.
4. Appendices A and B, when completed, will be the subject of Criminal Procedure and Investigations Act 1996 (CPIA) requirements.
5. The working group continues the development of these documents for possible inclusion in National File Standards.
6. The working group will continue to develop a national "Stafford Statement"* to address concerns raised by a number of victim support organisations.

2. Intention

This paper is to inform the Criminal Justice Co-ordination Committee of the work and associated recommendations to ensure consistency of approach when extracting digital data from the devices belonging to complainants and witnesses during the course of an investigation.

3. Background

Digital devices, including smart phones and tablets are continuing to evolve, with ever increasing capacity to store information. When combined with the developing potential for cloud storage, this modern reality poses an unprecedented challenge to policing in terms of investigations where such stored information may contain evidence relating to criminal offences. Enquiries into digital media which were once only employed in exceptional cases are now commonplace, substantially increasing the burden upon investigators, particularly when attempting to discharge their responsibilities under CPIA disclosure. As well as devices belonging to suspects, reasonable lines of enquiry now frequently extend into the devices of complainants and witnesses particularly when parties are known to each other.

Policing practices have been adapted at local levels in an attempt to manage this developing situation, but as a consequence the approach has become divergent between individual forces. The scoping exercise by the working group has shown that there is a lack of clarity concerning the powers under which officers are seizing and interrogating these devices, as well as a fragmented approach to informing complainants and witnesses how their personal data will be extracted, stored and managed. Forces also differ as to whether they request consent from those individuals concerned and, if obtained, how this consent is recorded, managed and ultimately disclosed throughout the course of an investigation.

Third party material is acquired from a number of sources and can be vital in the pursuance of reasonable lines of enquiry. Recent CPS guidance highlights the process to be followed in this regard. Again, consent is needed when third party material is required. However, there is no formal process to do this.

Therefore, in both these cases there is a clear need to provide guidance for police investigators to ensure that the rights of individuals are proportionately balanced against the needs of the case. National clarity and consistency concerning these processes will help promote a fair and transparent judicial process with due regard for individual privacy and freedoms as enshrined in human rights legislation. The working group has identified four main areas of risk through its scoping work which are detailed as follows:

*The reference to 'Stafford statement documents' arises from the case of R(B) v Stafford Crown Court (2007) which stated a complainant's article 8 rights must be considered when it comes to disclosure. Complainants should be informed of any request from the defence for their records, and be given an opportunity to make representations at a hearing.

4. Legality

Following advice from Counsel relying on Section 19 Police and Criminal Evidence Act, which allows a constable to

seize items that may be evidence of an offence is unlawful in circumstances involving witnesses or complainants. It was confirmed also that there is no legal basis in which to seize or extract information. In order to take possession of a complainant or witnesses' device the only credible solution is consent. However, it has been argued that consent cannot form any basis in which to extract that information as this is not true consent as there is only a very small window in which to withdraw that consent before any data is extracted, when there is no opportunity to withdraw it as the police are thereafter bound by the legal position of having to retain material in line with CPIA*.

The same can be said for 3rd party material and as such consent is the only basis in which we can gain access to such material.

It is accepted that this position carries a degree of risk, since it cannot rely on any current legislation and any direction through case law is likely to be in the long term. The focus now being brought to bear on our practice in this area has culminated in the critical need for police service to adopt a nationally consistent position, with the risk of inaction now outweighing any uncertainty concerning our proposed guidance.

5. Consent

It is vital that complainants and witnesses are clear as to what they are consenting to at the outset of an investigation and are kept up-to-date of any subsequent changes to how their data may be used during the course of that investigation. When information, data or material is to be disclosed to the defence, and the defendant before or during trial, the subject person of the information, data or material must be given early notice and given the opportunity to present to the court a reason why this data should not be disclosed.

Appendix A provides clear, unambiguous information on why the data is required, what we do with it and how we store and protect. Appendix B provides specific technical information and requires a complainant or witnesses signature.

6. Disclosure

With varying practices being used by forces, it has become apparent that the processes, particularly involving those where consent by complainants is either given or refused, are not always being adequately disclosed as part of the police duty under the CPIA such as appropriate scheduling on the MG6 series of documents. Clearly this has the potential to undermine cases that proceed to court.

7. Consistency

The overarching risk to policing is that of an inconsistent approach through lack of guidance. Initial enquiries with all forces have identified that the practices around the country can vary greatly. Some forces seek blanket consent for downloading information, whereas others permit the complainant to exclude specific categories, e.g. photographs. Some forces issue a detailed notice to complainants and obtain signed consent, whilst others rely on that consent being captured within the body of a statement. Finally, some forces do not seek consent at all, opting instead to simply inform a complainant about what will happen.

Given the strategic drivers behind this piece of work and the current improvements being implemented under the National Disclosure Improvement Plan, this is not a situation that should be tacitly approved. Failure to disclose and potentially illegal or unethical process will cause grave issues for Policing.

*All information recovered in the course of a criminal investigation must be handled and stored securely in accordance with the provisions of the Data Protection Act 2018, CPIA1996 and the MoPI 2005.

8. Recommendations

The working group have identified the best method, in the circumstances, to inform complainants and witnesses of the process that will be undertaken concerning their digital devices and the need to access 3rd party material. Following Counsel and Information Commissioner's advice the working group advocate adopting an ethical

approach and providing complainants and witnesses with comprehensive information in terms of how we extract, store, retain and ultimately disclose their data.

Two documents have been drafted which have been included as appendices. They consist of an information letter for complainants and witnesses and a digital processing notice. It is envisaged that, if agreed, a final version of these can potentially be developed to become part of the National File Standards.

The Criminal Justice Co-ordination Committee is asked to consider the following recommendations:

1. All forces to seek consent from complainants and witnesses after supplying supporting information (Appendix A) and conducting a two-part discussion for seeking 3rd party material, taking digital devices **and** extracting data.
2. The use of Sec 19 PACE to secure complainants and witnesses digital devices is to cease with immediate effect.
3. Consent to seize devices is to be recorded on the appropriate document (Appendix B) and forces are directed to use this attachment and any adaptations are to be minor (use of Force logo/website etc.)
4. Appendices A and B when completed are to be subject of disclosure considerations in line with CPIA.
5. The working group continues with the development of these documents in collaboration with the College of Policing for inclusion in the National File Standards.
6. The working group will continue to develop a national "Stafford Statement"* to address concerns raised by a number of victim support organisations.

Task and Finish Working Group

Table 1.

Full Name	Department/ Organisation
ACC Burton	NPCC Disclosure (Task and Finish Group lead)
CC Gareth Wilson	NPCC Investigations
ACC Emma Barnett	NPCC Victims and Witnesses
John Beckwith	NPCC Digital Forensics
Kate Anderson	CPS
Meagan Mirza	ICO
Mark Jones	ICO
Wei Lynn Ng	ICO
Mark Davies	NPCC Digital Forensics
Ian Grant	NPCC Digital Forensics
Andrew Wadey	Metropolitan Police
Sian Thomas	Metropolitan Police
Gail McCoo	Surrey Police
Helen Bayliss	Surrey Police
Chris Hampshire	Surrey Police
David Johnston	NPCC Data Comms
Faye Maxted	Survivors Trust
Libby Potten	College of Policing

Appendix A

Digital device extraction and request to access third party material – information for complainants and witnesses

We understand that a request to obtain personal or private information, either from your mobile telephone, digital device or another person or organisation who holds records about you, has the potential to cause anxiety. The purpose of this document is to explain why we may be making a request, what will happen to your data and to address some of the concerns that you may have. A list of other agencies who may offer support and advice is included at the end of this information sheet.

You may be asked to give your consent to download data from your device, such as text messages and emails. You may also be asked to give your consent for the police to approach other organisations who hold information about you. We refer to this as “third party material”. We will explain to you why we need to do this.

Digital Devices - why we may need to look at your ‘phone and other digital devices

The police have a responsibility to investigate crimes and gather all evidence that may be **relevant** to the case. “Relevant” means anything that has some bearing on any offence under investigation, or on the surrounding circumstances of the case. Investigations have to be thorough and the police have a legal duty to follow all reasonable lines of enquiry. These lines of enquiry will depend upon the individual circumstances of each case.

Mobile phones and other digital devices such as laptop computers, tablets and smart watches can provide important relevant information and help us investigate what happened. This may include the police looking at messages, photographs, emails and social media accounts stored on your device. We recognise that only the reasonable lines of enquiry should be pursued to avoid unnecessary intrusion into the personal lives of individuals.

You may be able to tell us where you think the relevant information is on your phone or other digital devices, or you may not. You will be asked about this during the initial stages of the investigation. This process may also be applied to the suspect’s mobile phone and other relevant devices in order to establish if there is any data that might be relevant to the case.

Digital Processing Notice

Before obtaining data from your device(s), we will ask for your consent and request you sign a form called a 'Digital Processing Notice'. The form provides you with important information about how we store and protect the data obtained from your device(s) and it is important that you read it carefully. You will be given a copy of this form and we will retain it in line with legislation.

What we do with your digital device?

There are essentially 3 levels of examination that can be applied to a device and this will affect what data is obtained. The data that can be extracted may vary by handset and the extraction software used. You will be provided with further information by the officer dealing with your case. However, the following broadly describes the level of extraction:

- **Level 1** – called a “logical extraction”. This may provide almost all of the data you could see if you were to turn on the device and browse through it. It will **not** normally extract data that has been deleted from the device.
- **Level 2** – either a “logical” extraction using selected tools in a laboratory environment or a “physical” extraction, which recovers a copy of the data held on the memory chip of the device. “Physical” downloads can extract deleted data, although capabilities vary depending on the nature of the device and the operating system.
- **Level 3** – these are usually expert and bespoke methods to tackle complex issues or damaged devices.

Some technology will not be able to obtain material using parameters such as a specific time period, meaning even though we may only consider a limited number of messages relevant to the investigation, the tool may obtain all messages.

Depending on the nature of the investigation, data from your device may be downloaded at the police station and your device returned to you, or we may need to send it to a digital forensics laboratory, which will mean that we will need to keep your device for a longer period, including until the end of any criminal proceedings.

The investigating officer will explain to you what level(s) of examination will be applied to your device and how long we are likely to keep your device for.

The Crown Prosecution Service (CPS) is the body responsible for prosecuting criminal cases investigated by the police in England and Wales. Evidence gathered by the police will be handed over to the CPS, who prepares the case for court. Sometimes the CPS will advise the investigating officer about what data should be examined before a case is charged, and sometimes they may ask for further investigations to be conducted after a case has been charged.

This process can take some time and it may be that we need to keep your phone and any other devices for several months, or we may request it from you again at a later stage. We may be able to supply you with an alternative mobile phone.

What happens to the data obtained from your device?

Once data has been downloaded and reviewed, we divide the material into different categories:

- 'Used' material – this is data that we want to use as evidence in court if the case goes to trial;
- 'Unused' material – this means that it is relevant but does not form part of the evidence that the prosecution wants to rely on. If unused material may undermine the prosecution case, or assist the defence then it must be provided to the defence if there is to be a trial; and
- Material which is not relevant because it is not capable of having any bearing on the case - this is not used either as evidence, or disclosed as unused material but will be retained until the conclusion of criminal proceedings.

Data obtained from your mobile phone or other digital device may be used as evidence to support the prosecution case, which means that it will be shown to the suspect/defendant and used in court. If unused material could assist the defence or undermine the prosecution case then it will also be shown to the suspect/defendant.

If data obtained from your device needs to be shown to the suspect/defendant, either as evidence or as disclosed unused material then we will inform you of this.

In some cases the court will make an order for you to release data; but this is rare and before this happens you will be given an opportunity to make representations at court.

What happens if we find evidence of other criminal offences?

If information is identified from your device that suggests the commission of a separate criminal offence, other than the offence(s) under investigation, the relevant data may be retained and investigated by the police. This data may be shared with other parties including, for example other police forces or a court in any criminal proceedings.

If your device contains information that may assist in the prevention or detection of crime, or protecting the vulnerable, then the police may process and retain this information on our intelligence management system and/or share that information with relevant parties/agencies, including other police forces or government agencies, including those outside of the UK.

Third Party Material

Other organisations may hold information about you which it is reasonable to believe may be relevant to the offences(s) under investigation. You will be asked for your consent to seek access to specific information that might have a bearing upon the investigation and any trial that might follow in the event that someone is charged, together with an explanation of why this is necessary.

If information about you is obtained from a third party, this will be reviewed by the police who will decide if it is relevant, and if it will be “used” or “unused” material in the prosecution (see above). The defence will only have access to such parts of the material to ensure that the trial is fair.

We will inform you if disclosure of third party material relating to you needs to be made during the course of the case.

What happens if I refuse consent for the police to access my data or information held about me?

If you do not provide consent for the police to access data from your device, or to access information held about you by a third party you will be given the opportunity to explain why. If you refuse permission for the police to investigate, or for the prosecution to disclose material which would enable the defendant to have a fair trial then it may not be possible for the investigation or prosecution to continue.

If a prosecution is able to continue then the defence representatives will be told of your refusal and a judge may order disclosure to take place. If this happens, you will be given the opportunity to make representations to the court about the reasons why you object.

Further questions or complaints

If you have any further questions or you have a complaint, please speak to the investigating officer in charge of your case.

Alternatively, you can contact our Professional Standards Department (insert force details).

If you have a complaint regarding how the police have handled your data either from your device(s) or a third party, you have the right to complain to the Information Commissioners Office, who are the UK's independent body set up to uphold information rights. They can be contacted through their website on <https://ico.org.uk/make-a-complaint/> or 0303 123 1113.

National Support Agencies

- Victim Support [0808 1689 111](tel:08081689111)/[0808 1689 293](tel:08081689293) or www.victimsupport.org.uk
- Rape Crisis [0808 802 9999](tel:08088029999) or www.rapecrisis.org.uk
- SAMM [0845 782 3440](tel:08457823440) or [0121 472 2912](tel:01214722912) www.samm.org.uk
- Citizens Advice Bureau www.citizensadvice.org.uk
- UK Government Website www.gov.uk/find-a-community-support-group-or-organisation

[INSERT YOUR FORCE LOGO HERE]

Appendix B

[INSERT FORCE] DIGITAL PROCESSING NOTICE

Crime Reference number:

The police request your consent to take possession of your mobile phone or other digital device (laptop, iPad etc.) for the purpose of extracting information considered to be relevant to the investigation that you are involved with.

This form describes our data protection and safe storage responsibilities. Separate forms will be used for each device requiring examination. You will be provided with a copy of this form and it will be retained by the police until the conclusion of any related criminal proceedings.

This notice must be served alongside the information document entitled “Digital device extraction and requests to access third party material – information for complainants and witnesses” which explains the reason the police are requesting your digital devices(s), and how the data extracted may be used.

Please contact the investigating officer in your case should you wish to discuss further how we may use your data.

All information recovered in the course of a criminal investigation will be handled, stored and retained securely in accordance with the provisions of the Management of Police Information Act (MoPI) 2005. Further information on MoPI and other professional practice information can be found at the College of Policing Website (www.college.police.uk ► “APP” “Information Management”).

We also have a duty to retain certain information. The retention period of the data we collect from your device will vary depending upon the severity of the offence investigated.

The officer investigating your case can print out relevant parts of MoPI for you if you have concerns, or email you the link to the appropriate parts of the website. This document can also be emailed with the following links: [MoPI 2005](#)

[Retention period](#)

“APP” ► “Information Management” ► “Retention, review and disposal” ► “Review schedule”

The police are under a legal obligation to pursue all reasonable lines of enquiry. To enable us to meet this obligation we are requesting access to your device and data on it as set out below.

In order to investigate the crime you are involved in, the police intend to extract the following data categories from the device e.g. call data, messages, email, contacts, applications (apps), internet browsing history etc.:

.....
.....
.....
.....
.....

(Continue on a separate sheet if necessary.)

It is the intention of the investigating officer to use the following, or a combination of the following level of extraction. Should an alternative level of extraction become necessary in order to successfully recover data, the investigating officer will contact you with an update and further consent may be required.

Level 1 – called a “logical extraction”. This provides almost all of the data you could see if you turn on a device and browse through it. It will **not** normally extract data that has been deleted from the device.

Level 2 – either a “logical” extraction using selected tools in a laboratory environment or a “physical” extraction, which recovers a copy of the data held on the memory chip of the device. “Physical” downloads can extract deleted data, although capabilities vary depending on the nature of the device, and operating system.

Level 3* – these are usually expert and bespoke methods to tackle complex issues or damaged devices.

Each of these levels may extract data in addition to that listed above by the investigating officer. Additional data extracted but which is not relevant will be securely stored as described above.

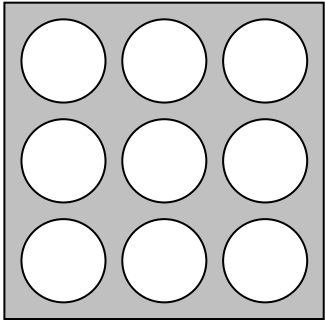
The investigating officer will explain the technical capabilities or restrictions relating to the above level of extraction. This could, for example relate to whether the methods used are compatible with your device and what data can, or cannot be extracted.

The level of extraction will determine how long we may need to retain your device. The investigating officer will explain how long this is likely to be in your case.

*Although great care will be taken to avoid this, Level 3 extractions may result in damage to the digital device, or permanent loss of data.

Device Details (to be completed by investigating officer):			
Exhibit Ref:			
Telephone No.:			
Make/Model No.:		Memory Card Present:	Yes ☐ No ☐
Device PIN Code:			
If alternative lock methods are present (i.e. fingerprint/face or iris) please ask complainant/witness to disable these in advance.			
General Description of Condition: (i.e. damage or faults, last used)			

Device Pattern Lock
(indicate beginning and end)



I have been given the “Digital device extraction and requests to access third party material – information for complainants and witnesses” form. I understand why the police are requesting my digital device and access to the data on it. I understand the process used to extract that data and I understand all relevant data (as determined by the investigating officer) will be handled, stored and retained as set out above. I consent to police:

Taking possession of my device and downloading data*

Requesting access to any relevant third party material*

The investigating officer will contact me if any of my data is to be disclosed to any suspect, or their defence representative.

(*delete as required)

Full Name:	
Address inc. postcode:	
Telephone Number:	
Owner / User of device signature:	
Age (If under 18):	Date:

The police will not disclose extracted material to any party, including parents/guardians, other than as required for the purpose of criminal proceedings or to comply with a legal duty.

Ordinarily, the police seek the involvement of a parent/guardian of a complainant or witness under the age of 18. Any objection to the police informing a parent/guardian of this request will be recorded, together with any reasons given. The police will try and comply with your wishes but there may be circumstances when it will not be possible to do so.

Investigating Officer*			
Name:		Force ID Number:	
Rank/phone number:		Location/Unit:	
Signature:		Date:	

Data Controller:	Chief Constable of
Information Commissioner's Office Registration Number:	
Data Protection Officer Address:	[Insert force website.]
Should you wish to make a complaint in respect of how your information and data has be handled by the police, you can contact the Information Commissioners Office.	https://ico.org.uk/make-a-complaint/ 0303 123 1113

**Note for investigating officer: Please ensure a copy of this is provided to the owner/user of the device.*