HEDDLU GOGLEDD CYMRU
Gogledd Cymru diogelach

NORTH WALES POLICE
A safer North Wales

Response Date: **04/01/2019**

2018/1166 - Victims Consent

In response to your recent request for information regarding;

Your force's use of consent statements when requesting, accessing, analysing and disclosing personal information from complainant's of sexual offences. Specifically, I am asking the following:

1. Does your force collect digital information from devices belonging to complainants of sexual offences? Yes

If yes, please provide:

i. **The legal basis under which you are doing this -** Section 19 PACE

ii. **Copies of any policy or guidance in relation to this practice –** North Wales Police do not hold this information.

2. Does your force seek consent from complainants of sexual offences when requesting, accessing, analysing, or disclosing digital or personal information either from them or records from a third party organisation relating to them? For the avoidance of doubt, records from third party organisations includes but is not limited to medical records, counselling records, local authority records, educational records or rape crisis centre records. Yes - consent is sought from victims and suspects of sexual offences when accessing social media accounts.

If yes, please provide:

i. **A copy of the consent form/s or statement/s you use and require them to sign to show their consent**

Please see attached

ii. **A copy of any information provided to complainants about this process –** no information held

iii. **A copy of your policy or guidance in relation to this practice -** no information held

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 31/12/2018

Consented Access Notice

HEDDLU GOGLEDD CYMRU
Gogledd Cymru diogelach
NORTH WALES POLICE
A safer North Wales

The North Wales Police seeks your authority to access your device or account(s) and the information contained within for the purposes set out below. The information recovered may be used in evidence should a prosecution be authorised. This notice outlines what information will be accessed and the reasons for this access, giving you the opportunity to explicitly consent to this processing.

All personal information provided to North Wales Police will be processed in accordance with our policing purposes as defined by "Authorised Professional Practice" protocol, which states;

> *'Any personal information obtained by North Wales Police will be processed in accordance with the Data Protection Act 1998 and may be held in manual or electronic form. It will be processed in accordance with North Wales Police's broad policing purposes of preventing and detecting crime; protecting life and property; preserving order; maintaining law and order and rendering assistance to the public. It will be securely deleted when no longer required.'*

Whilst the sole intention of this request is to upload the information in line with our policing purposes above, due to our forensic procedures our systems may collect other information from your device or account. For example, where an investigation requires access to a single text message that may be held on your device, our system may upload all text messages held on that device.

All information recovered in the course of a criminal investigation will be processed in accordance with the provisions of the Criminal Procedure and Investigations Act 1996 (CPIA) as amended by the Criminal Justice Act 2003.

North Wales Police do not speculatively interrogate devices. However if during the course of the examination information is identified that may amount to a criminal offence, then we, North Wales Police, will retain that data for the purpose of investigating whether an offence has been committed. This may include disclosure of relevant information from your device or accounts to other parties including other government agencies, suspects, legal teams and to a judge and jury. The evidence will also be assessed for intelligence value and may be processed for the purposes outlined above.

Access to accounts will only be authorised for the period necessary to review and obtain any evidential material. Once a review has been completed the authorisation will be cancelled and you will be notified that ownership of the accounts has been returned to you. North Wales Police will not access any accounts without a lawful authorisation.

Failure to Consent

Failure to consent to this notice may result the application of an account preservation order being served upon the relevant service providers.

Accessing Accounts following release from custody.

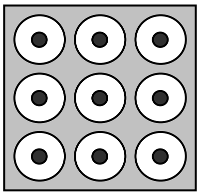
Should you or another who has been caused by you, access your accounts following notification that the accounts are being investigated by police and have been secured for the purposes of doing so, may be liable for arrest and prosecution for offences of Obstruction and Perverting the Course of Justice.

Reference Number: (e.g. Inc No. Crime No.)			
Officer In Case*			
Name:		**Rank:**	
Officer In Case Signature:		**Date:**	
Supervising Officer*			
Name:		**Rank:**	
Supervising Officer Signature:		**Date:**	

Note for Officers: Please ensure a copy of this form is provided to the Owner/User of the device(s) or account(s).

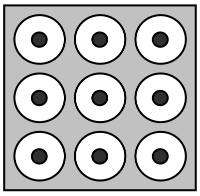
Device

Device Details

Make/Model No.:				**Device Pattern Lock** (indicate beginning and end)	
Telephone No.:		**Data Card:**	**Yes** ☐ **No** ☐		
IMEI No.:					
SIM PIN Code:		**Device Pass Code:**			
Alternative Lock Methods:	Biometrics ☐ Please remove any biometric locks.	Other ☐			
General Description of Condition:					

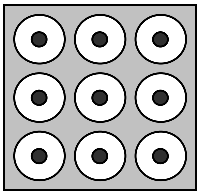
Device

Device Details

Make/Model No.:				**Device Pattern Lock** (indicate beginning and end)	
Telephone No.:		**Data Card:**	**Yes** ☐ **No** ☐		
IMEI No.:					
SIM PIN Code:		**Device Pass Code:**			
Alternative Lock Methods:	Biometrics ☐ Please remove any biometric locks.	Other ☐			
General Description of Condition:					

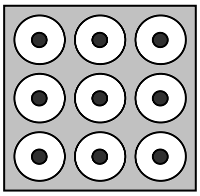
Device

Device Details

Make/Model No.:				**Device Pattern Lock** (indicate beginning and end)	
Telephone No.:		**Data Card:**	**Yes** ☐ **No** ☐		
IMEI No.:					
SIM PIN Code:		**Device Pass Code:**			
Alternative Lock Methods:	Biometrics ☐ Please remove any biometric locks.	Other ☐			
General Description of Condition:					

Device

Device Details

Make/Model No.:				**Device Pattern Lock** (indicate beginning and end)	
Telephone No.:		**Data Card:**	**Yes** ☐ **No** ☐		
IMEI No.:					
SIM PIN Code:		**Device Pass Code:**			
Alternative Lock Methods:	Biometrics ☐ Please remove any biometric locks.	Other ☐			
General Description of Condition:					

Account(s)

Account Details

Service Provider	Account Name	Log on Details	Password
e.g. Hotmail	*John Smith*	*anyone@hotmail.co.uk*	*ABC1234*
e.g. Facebook	*Paul Williams "Paul Wills"*	*paul.williams78834@examplegmail.com*	*wills78xzA*
e.g. Instagram	*Profile name: Chloe Jones Username: "Chloe_Jones91x"*	*chloej91@exampleoutlook.co.uk*	*Chloe*91*
e.g. iCloud	*Dave Matthews*	*Dmatthews987@exampleicloud.com*	*icloud987*
MAKE SURE WRITE	PASSWORDS ARE CASE SPECIFIC CLEARLY IN	I.E. UPPERCASE/lowercase BOXES BELOW	**PLEASE DOUBLE CHECK** THIS LINE

I, as the owner of the information, having read and understood the above statement, explicitly consent to North Wales Police accessing the requested material as outlined above, from my device(s) and or account(s). **I consent that the Police may change any logon email, password and user settings to enable secure access to my device(s) or account(s) and these will be reset to the original settings once data has been obtained and recorded, if no evidence of criminality is identified.**			
Information to be accessed and reason access is required. **Be clear as to what is being authorised.** **i.e. Specific messages between individuals, Dropbox Account, iCloud etc**			
Facebook Account Archive Downloads ONLY (This box only applies to Archive downloads) **Be specific, what has been authorised by the account owner/user. It is possible to select time/date ranges, messages, images, videos etc. Only what is relevant.**			
Full Name:			
Owner / User of Device Signature:		**Date:**	
As an Appropriate Adult, acting on behalf of the above named, I accept that I have read and understand the above statement and I also explicitly consent to North Wales Police accessing the requested material, as outlined above, from the device(s) and or account(s).			
Appropriate Adult: Full Name		**Relationship to the owner.**	
Signature		**Date:**	

Retention Period: The retention period of the information we collect from your device or account(s) will vary depending upon the severity of the offence investigated. In this case, it is likely that your information will relate to the following category and retention period:

Crime / Investigation Type:	**Retention Period**	**Tick √**
Serious Offences [e.g. murder, rape, indecent assault, child abuse, terrorism, threats to Kill, etc]	**100 Years**	☐
Other Sexual / Violent Offences [e.g. ABH, violent disorder, affray, exposure, voyeurism, etc.]	**10 Years**	☐
Other Offences [e.g. theft, criminal damage, minor public offences , etc]	**7 Years**	☐

To be completed following the conclusion of the account review.

I confirm the subject has been informed that North Wales Police have reviewed the authorised accounts and ownership has been handed back, no further access will be made.			
Subject Informed		**Time/ Date**	
Informing Officer Signature:		**Officer No**	

Appendix A

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 your 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 111/0808 1689 293 or www.victimsupport.org.uk

Rape Crisis **0808 802 9999 or** www.rapecrisis.org.uk

SAMM 0845 782 3440 or 0121 472 2912 www.samm.org.uk

Citizens Advice Bureau www.citizensadvice.org.uk

UK Government Website www.gov.uk/find-a-community-support-group-or-organisation

Appendix B

[INSERT FORCE] POLICE 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 legal 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.

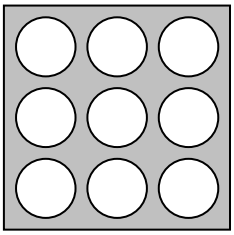
☐ **Level 3*** – these are usually expert and bespoke methods to tackle complex issues or damaged devices.

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 Officer In Case):				
Exhibit Ref:				Device Pattern Lock (indicate beginning and end) 
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)				

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 devices.

National Police Chiefs' Council

Consent for Digital Downloads during the Course of an Investigation

16 January 2019 / Agenda Item: Regional

Security Classification Papers cannot be accepted without a security classification in compliance with the Government Security Classification (GSC) Policy (Protective Marking has no relevance to FOI):	OFFICIAL-SENSITIVE
Freedom of information (FOI) This document (including attachments and appendices) may be subject to an FOI request and the NPCC FOI Officer & Decision Maker will consult with you on receipt of a request prior to any disclosure.	
Author:	ACC Jeremy Burton
Force/Organisation:	Surrey Police
Date Created:	19/11/2018
Coordination Committee:	Criminal Justice Coordination Committee
Portfolio:	Disclosure Portfolio
Attachments @ para	App A
Information Governance & Security In compliance with the Government's Security Policy Framework's (SPF) mandatory requirements, please ensure any onsite printing is supervised and storage and security of papers are in compliance with the SPF. Dissemination or further distribution of this paper is strictly on a need to know basis and in compliance with other security controls and legislative obligations. If you require any advice, please contact npcc.foi.request@cru.pnn.police.uk https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework#risk-management	

1. EXECUTIVE SUMMARY

1.1 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".

1.2 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.

1.3 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 Criminal Justice Coordination Committee (CJCC), 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.

1.4 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 on 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.

1.5 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.

1.6 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

2.1 This paper is to inform the Chief Constables' of the work and associated recommendations to ensure consistency of approach when extracting digital data from the devices belonging to victims and witnesses during the course of an investigation.

3. BACKGROUND

3.1 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 victims and witnesses particularly when parties are known to each other.

3.2 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.

3.3 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.

3.4 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

4.1 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. It 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 and 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*.

4.2 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.

4.3 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

5.1 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.

5.2 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 the complainant or witnesses signature.

6. DISCLOSURE

6.1 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

7.1 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.

7.2 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

8.1 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.

8.2 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.

9. APPROVAL OF THE COORDINATION COMMITTEEE

9.1 This paper was agreed by the Chair of the Criminal Justice Coordination Committee on the 14 December 2018.

10. DECISIONS

10.1 Chief Constables' Council 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.

Assistant Chief Constable Jeremy Burton
Surrey Police
NPCC Lead for Disclosure