



Mobile Fingerprint Identification Policy (Surrey and Sussex) (1191/2026)

Abstract

Using provisions under Section 61 (6A) of the Police and Criminal Evidence Act 1984 (PACE) and Code D, in order to ascertain identity, the Mobile Fingerprint Devices (MobileID) allow the police officer to take an individual's fingerprint (under certain criteria) and check it against relevant law enforcement databases. The taking of a fingerprint must not become the first mechanism for establishing identity and usual practices and protocols apply in the first instance; no new power to detain is provided. The devices / software are not capable of capturing the biometric data used to research the database; no fingerprint data are retained after the search. Mobile Data Terminals are fully auditable for any legitimacy considerations.

Policy

1. Introduction

1.1 The purpose of this document is to explain the legal framework for the operational use of Mobile Fingerprint Identification Devices (referred to as MobileID going forward) technology under which England and Wales Police Forces operate. The procedures must be considered a minimum standard for using MobileID.

2. Scope

2.1 The purpose of this policy is to ensure MobileID is used correctly so that Surrey Police and Sussex Police will gain maximum benefit from the operational use of the devices, and that all police officers coming into contact with the equipment are able to comply with legislation and Force requirements to safeguard its integrity.

3. Policy Statement

3.1 Surrey Police and Sussex Police are committed to making the best use of its resources and to ensure that they take full advantage of new technology.

Procedure

1. Introduction

1.1 The implementation of the MobileID to the toolkit for frontline police officers, is seen to be a key enabler of ensuring that we are dealing with the right people, at the right time, in the most efficient manner. Police officers must be clear on the parameters around the use of the mobile fingerprint reader in order to maintain public confidence in policing.

2. Legislation

2.1 The taking of fingerprints is legislated in the Police and Criminal Evidence Act 1984 (PACE).

Section 61 (6A) of PACE and Code D provides the legal power for the use of MobileID, for which two criteria are now required:

“the constable reasonably suspects that the person is committing or attempting to commit an offence, or has committed or attempted to commit an offence

AND

(a) the name of the person is unknown to, and cannot be readily ascertained by the constable

OR

(b) the constable has reasonable grounds for doubting whether a name furnished by the person as their name is their real name”.

3. National Decision Model (NDM)

3.1 Before police officers consider the use of the MobileID devices, they are reminded that there are other established methods of ascertaining identity which include Driving Licence, passport and so on. The use of the MobileID must not be the first option considered and you are reminded that you are likely to be asked to account for your use. Therefore, the decision to take fingerprints must be considered in line with the NDM.

3.2 Police officers may check fingerprints without specific consent from the individual.

3.3 It should be noted that the devices will search the fingerprint databases and return a result based on certain criteria; the result returned will show a level of ‘confidence’ in the returned results and the police officer should always be careful to note that the result may not be conclusive. Further action, in the event of an inconclusive response, must always be considered carefully.

3.4 Although no consent to take a fingerprint is required, police officers are reminded that those that might fall into a ‘vulnerable person’ category (for example, age / mental capacity / disability) must be treated within the same lawful parameters and with the same respect as per usual interactions for those groups.

4. Operational guidance

4.1 Before exercising this power, the police officer must ensure that the individual is informed of the nature of the suspected offence, why they are suspected of committing it, and then give the individual the opportunity to establish their identity.

4.2 If the police officer should then decide that the individuals' name is unknown and cannot be readily ascertained (i.e., individual refuses to provide it; identification document is insufficient or there are reasonable grounds to doubt that the name given is their real name), then this must be explained clearly, and the subsequent possibility of the fingerprint procedure explained. The officer must give a further opportunity for the person to furnish details.

4.3 If no details are provided, or there remains reasonable doubt, then the fingerprint procedure can be commenced (please see 'Health and Safety' below).

4.4 It is the police officer's responsibility to ensure that the circumstances and their decision is noted in their (e)PNB. This must include:

The steps taken to allow the individual to provide their correct identity;

Any ID details already provided;

The reasons why these details are suspected to be false;

What efforts have been made to allow the person to validate the details provided.

4.5 The results of a MobileID search may make an arrest for the suspected offence unnecessary and enable the offence to be disposed of without arrest, for example, by summons / charging by post, penalty notice or words of advice. The results may also eliminate the individual from further enquiries entirely.

4.6 Fingerprints taken under this power will not be retained after they have been checked. The Pronto software will not store the fingerprints taken but will record the fact that they were checked against the database.

4.7 Before concluding any encounter with an individual that has committed, or is suspected of having committed an offence, police officers must be completely satisfied that the identity of the individual is fully and accurately established. Individuals must also be advised that their fingerprints have not been retained or recorded and used only for the purposes of the database search.

4.8 All relevant legislation, including the Human Rights Act 1998, the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR) and the Computer Misuse Act 1990 are applicable. Police officers are reminded of their duty to remain informed of these by way of normal on-going professional development (for example, College Learn (NCALT) eLearning or officer briefing packages).

5. Health and Safety

5.1 Before the check is undertaken, police officers should consider a number of Health and Safety / hygiene factors. Where necessary, risk assessments should be updated to consider the use of the device.

5.2 Clearly there is a certain proximity required with the individual in order for the fingerprints to be taken and scanned. Police officers should remain situationally aware and make the decision to use the mobile reader devices only when they are clear that there is no immediate or apparent risk from the individual, those around them, or the environment.

5.3 Unless there are significant practical or time critical reasons why this cannot be completed, at the beginning and the end of every check the device must be wiped clean and dry with an appropriate anti-microbial and anti-viral wipe (see section 8.1 below – Dead Bodies and Crime Scenes).

5.4 Police officers are reminded to adopt safe working practices when dealing with any member of the public who poses a risk from infectious disease. If the subject has any kind of injury that has resulted in bleeding, or if their hands are contaminated with any other body fluids, the use of the device must be considered carefully in the first place. If deemed necessary, first-aid wipes must be used on the subject prior to providing their fingerprints. In these circumstances, it is also imperative that the device is wiped clean and dry with an appropriate anti-microbial and anti-viral wipe post-check.

5.5 Mobile devices use a mobile phone signal to transmit data and, as such, can pose a potential risk where used in circumstances where that method might be problematical. For example, this could include incidents involving suspected 'Improvised Explosive Devices' or where the individual is on a petrol filling forecourt.

6. Use of Force

6.1 Code D - Revised Code of Practice for the identification of persons by police officers (4.6) - provide police officers with the power to take a fingerprint by force; however, this is not recommended in using MobileID and officers should revert to other options in these circumstances in order to avoid injury e.g., arrest if appropriate.

6.2 Use of Body Worn Video (BWV)

Where a police officer is equipped with BWV they MUST record the interaction, with exception of dead bodies, then record if for an evidential purpose.

6.3 In the unlikely event that force is used, the police officer must be able to demonstrate that the use of force was reasonable, justified, and proportionate. The police officer will ensure that they create a 'Use of Force' form before the end of shift. To reiterate, it is highly unlikely that you would be in a position where 'Use of Force' is a necessary option whilst using MobileID.

7. No offence of 'failing to provide a fingerprint'

7.1 PACE does NOT create an offence of 'failing to provide a fingerprint' and, therefore, an individual cannot be arrested for not providing a fingerprint only.

8. Instances where PACE powers are not required

8.1 PACE powers are not required for the use of Mobile Fingerprinting in the following circumstances:

- Where consent is freely given by the person whose fingerprints are required;
- Unconscious persons: In these circumstances the Mental Capacity Act 2005 is active, and the duty of care principles take priority;
- Dead Bodies: This scenario supports Section 5 (1) of the Coroners and Justice Act 2009 and the Police Service's duty to support HM Coroner in the identification of dead bodies. Police officers are reminded to give due consideration to their own personal health and safety when taking fingerprints from the deceased, and also mindful of impacts on potential crime scenes. Before using the devices at a crime scene, seek the authority of a senior officer / Crime Scene Investigator (CSI).

9. Fingerprint database enquiries

9.1 There are two fingerprint databases available via the search facility provided by the Pronto software. Although it is possible to only select one of the databases to search, it is strongly recommended that both databases be selected in order to complete a thorough fingerprint enquiry:

Ident1 (a database which contains all criminal biometric information for all unspent, recordable, criminal offences resulting from a conviction). Only police officers with 117 access assigned to their Pronto account will be able to review any Police National Computer (PNC) result returned. As with the standard PNC enquiry check, if the police officer is unable to identify the appropriate action required then enquiries should be made with the relevant support function.

The Home Office Immigration and Asylum Biometrics System (IABS) which holds biometric data for all visa / immigration applicants and asylum seekers until naturalised. This response may also include a photo of the person on record, further aiding identification.

Should police officers identify that the individual stopped and checked via mobile identification is (potentially) a person of interest to Home Office Immigration Enforcement then contact should be made immediately with the Command and Control Unit (CCU) which is staffed 24/7: (text redacted)

The interrogation of Immigration Enforcement Data by police officers is not advised; the data held by the CCU is complex and requires access to a variety of additional systems in order for immigration status to be fully understood. Taking action without having contacted CCU is not an appropriate use of the data retrieved.

10. Audit

10.1 When a biometric fingerprint search is conducted, the Pronto software will automatically stamp the users 'Shift' to highlight that this has taken place. As such, unless there are urgent and extenuating circumstances as to why it cannot be achieved, police officers must not use another person's Mobile Data Terminal (MDT) to conduct the check.

10.2 Should there be any urgent and extenuating circumstances, a 'Text Entry' must be added into the affected police officer's (e)PNB before the shift is ended to that extent.

10.3 There are currently no Force reporting requirements. In order to investigate and manage complaints, Supervisors can use 'Pronto Manager' to review use (via 'Biometric Search'), with reporting data available to relevant Force legitimacy Boards.

10.4 It is likely that the use of this device will attract community feedback. All searches conducted on the MDT Pronto software are recorded and details can be extracted for legitimacy reporting purposes.

11. Security and fault reporting

11.1 The devices are not functional without the police officer's MDT and the Pronto Biometric software installed. However, when not in use, devices should be stowed out of sight.

11.2 The devices will not be personal issue at the point of first introduction to the Forces. As such, additional care should be used to ensure they are stored appropriately in Fleet vehicles.

11.3 Lost or stolen devices must be reported on the Security and Breach Reporting Portal, to the local Single Point of Contact (SPOC) or the IT Service Desk and follow the Surrey Police and Sussex Police Information Security Policy (722) (Security Incident Management Procedure.)

11.4 Devices that are 'lost' may be able to be located by the use of recent user interactions and the serial number of the device in the database.

11.5 If the device should develop a fault, then users should report this to the local SPOC in the first instance.

12. Other considerations

12.1 The use of the mobile device to perform the check is subject to the usual mobile devices operating procedure as outlined in other relevant policy areas. This policy is seen as complimentary to the Force Issued Electronic Devices (Surrey and Sussex) (1177).

Team: Operations Command