Mobile Biometrics

Contents

Flowchart

Is identification required under:

- S61(6a) PACE / Code D
- Mental Capacity Act 2005
- S5 Coroners and Justice Act 2009

YES

NO → No Power exists to use Mobile Biometrics

S61(6a) The subject MUST be informed of:

- Offence for which they are suspected
- Why they are suspected
- The requirement to furnish their identity

Bodyworn video must be set to record

Checks should be made using the following BEFORE use of Mobile ID where appropriate/available:
NICHE
PARS

STOP if Identification achieved

Conduct mobile biometric scan against IDENT1 database ONLY

STOP if Identification achieved

Conduct mobile biometric scan against IABS database (immigration)

Ensure that an accurate record is made including:

Steps taken to allow the individual to provide their correct identity

Any details provided by the individual

Why the details are suspected to be false

What efforts were made to allow the person to validate the details provided

Policy Statement

Summary

West Yorkshire Police (WYP) use mobile biometrics to ensure that we are dealing with the right people, at the right time, in the most efficient manner. Use of this technology should be done so in a professional manner that maintains confidence in policing.

This policy explains the purpose of mobile biometrics, the legal requirements, and conditions of use, including health and safety and training required.

The use of mobile biometrics fingerprint scanners should be considered as a tool to assist with the identification of a person and should be used where other methods such as PARS and the checking of Niche image have been unsuccessful or unsuitable.

Significant engagement and consultation have taken place regarding mobile biometrics, internally with districts and departments and the Force's internal ethics committee and externally through Independent Advisory Groups (IAG) and social media.

Any use of the Mobile Biometric device must be recorded on Body Worn Video (BWV) and the recording transferred onto the Force video management system. Any use of Body Worn Video must be in accordance with the Body Worn Video policy.

Scope

This policy applies to all police officers and police staff.

Definition

Mobile Biometrics

- Biometrics is the technical term for body measurements and calculations. It refers to metrics related to human characteristics.
- Biometrics authentication is used in computer science as a form of identification and access control.
- The context of this document relates to the Police use of biometrics in a mobile environment, the obtaining of a fingerprint image for digital analysis and database search to identify an individual within the principles set out in the Police and Criminal Evidence Act 1984 (PACE).

Principles

Legal Requirements

Police Powers for the Use of Mobile Fingerprinting

- Before police officers consider the use of the Mobile Biometrics devices, they are reminded that there are other established methods of ascertaining identity which include checking of documents, including driving licence and passports, and checking available police systems such as Niche and PARS.
- The use of mobile biometrics must not be the first option considered and individuals are reminded that they are likely to be asked to account for their use.
- Therefore, the decision to take fingerprints must be considered in line with the National Decision Model.
- Section 61 of PACE of Police and Criminal Evidence Act 1984 and Code D provides the legal power for the use of Mobile Fingerprinting, two elements are required:
  - An offence must have been committed (or suspected); **and**
  - Either no name is provided OR the name provided is suspected to be false.
- The power under section 61(6A) of PACE allows fingerprints of a suspect who has not been arrested to be taken in connection with any offence (whether recordable or not) using a mobile device and then checked on the street against the database containing the national fingerprint collection.
- This power only relates to **constables.**
- Fingerprints taken under this power **cannot** be retained after they have been checked.
- Being able to confirm a suspect's identity 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.
- Before the power is exercised, the officer must:
  - Inform the person of the nature of the suspected offence and why they are suspected of committing it.
  - Give them a reasonable opportunity to establish their real name before deciding that their name is unknown and cannot be readily ascertained; or that there are reasonable grounds to doubt that a name they have given is not their real name.
  - Inform the person of the reason why their name is not known and cannot be readily ascertained; or of the grounds for doubting that a name they have given is their real name. Including, for example, the reason why a particular document the person has produced to verify their real name, is not sufficient.

- Ensure that more commonly used methods to check a person's identity have been undertaken, i.e. passport, drivers' licence, checks on Niche and PARS.
- Take all reasonable steps to explain the process, and gain cooperation.

Use of Force

- Section 61 PACE and Code D provide officers with the power to take a fingerprint by force by virtue of Section 117 of the Act. Before doing so, all the criteria listed (for taking the sample) must be met in full.
- Any use of force **must** be reasonable, justified and proportionate.
- In the case of force being used officers **must** complete a use of force form, this should be completed within current force protocols.
- PACE requires that when force is used the person is advised the reason for fingerprinting and the power used to obtain. This will be recorded in the officers PNB, along with the nature of the force used. This should state the data subject has been advised. The data subject should be fully debriefed by the officer as to how the data is processed.
- The Mental Capacity Act 2005 allows for the protection of a person who lacks the mental capacity to make decisions to protect themselves. Therefore an officer will be justified in conducting a biometric search to identify an individual, who is in need of immediate medical attention where their identification might assist in that treatment. Police have a duty to save life.

No Power of Arrest

- The PACE amendment **does not** create an offence of "failing to provide" and therefore a person cannot be arrested just for not providing a fingerprint only.
- Officers must record:
  - What offence is suspected to have been committed;
  - Any ID details already provided;
  - The reasons why these details are suspected to be false; and
  - What efforts have been made to allow the person to validate the details they provided.
- PACE powers are **not** required for the use of Mobile Fingerprinting in the following circumstances
  - Unconscious people when duty of care principles take priority (An example of this maybe where an unconscious person is found in public and immediate care is needed. The individual is taken to hospital and ID is required to contact immediate family and to allow for the provision of medication). In these circumstances it will fall to the officer to make a decision on if to utilise Mobile Biometrics, and who to release data to considering the provisions of the Data Protection Act, and the Duty of Care Provisions under the Mental Capacity Act 2005. It would clearly not be unreasonable to provide details to a medical professional under these circumstances to support the care of the individual; or

- Dead bodies where Coroners rules apply (Coroners and Justice Act 2009)).

- *West Yorkshire Police has made the decision that fingerprints **will not** be taken where the subject volunteers to provide if there is no legal power to obtain.*

Children and Vulnerable Adults

- There is no power under PACE to obtain fingerprints from anyone under the age of ten years of age, and they will therefore **not** be obtained under these circumstances.
- Where Biometrics are obtained from a Child (over 10), or a Vulnerable person, it is unlikely that an appropriate adult would need to be present for the procedure.
- If there are concerns that the subject could not understand the information provided to them it would be advisable to await the attendance of the appropriate adult, pursuant to subsections 61(7) and 61(7A) PACE.
- When dealing with an unconscious person, an officer's responsibility to preserve life, and ensure appropriate treatment will be the officer's primary concern.

Data Protection Act 2018

- The Data Protection Act 2018 (DPA) regulates the processing of personal data or sensitive personal data; whether processed on computer, CCTV, stills, camera or any other media. Any recorded image that captures an identifiable individual is covered by the DPA.
- The DPA comprises eight principles and data controllers have a legal obligation to comply with these principles. Principle 1 of the DPA (fair and lawful processing) requires upon request that the data subject must be informed of:
  - The identity of the data controller;
  - The purpose or purposes for which the material is intended to be processed; and
  - Any further information that is necessary for the processing to be fair.
- The Act requires this information to be made clear to those individuals whose personal data will be processed. Officers must ensure the individual having their fingerprint taken is fully briefed on the processing of their information.

European Convention on Human Rights

- Article 6 of the European Convention on Human Rights (ECHR) provides for the right to a fair trial.
- All searches using mobile fingerprinting can be used in Court proceedings, whether they provide information that is beneficial to the prosecution or the defence.
- They must be safeguarded by an audit trail in the same way as other evidence that is retained for Court.

- Article 8 of the ECHR is the right to respect for private and family life, home and correspondence. Forces are required to consider this article when dealing with recorded images, whether they are made in public or private areas.
- The guidance provided regarding compliance with the DPA applies equally to Article 8 of the ECHR and it is important that officers and staff follow this guidance to minimise the risk of non-compliance.

Public Sector Equality Duty

- The decision by a force to use mobile fingerprinting is considered as a function for the purposes of the Equality Act 2010.
- The Force must therefore be able to demonstrate due regard to the public sector equality duty. In order to do this, officers and staff must work with members of the public who reflect local diversity to ascertain any impact (positive or negative) that the use of mobile fingerprinting will have.

Searches

Immigration

- Mobile biometrics provide officers with an option to search for an individual on both the IDENT1 criminal record database and on the Home Office Biometrics IABS Immigration Database.
- Should officers identify that the individual stopped and checked via mobile identification and the data returned indicates they are a person of interest to Home Office Immigration Enforcement then contact **must** be made immediately with the Command and Control Unit (CCU).
- The search of the Immigration database is a method of confirming the identity of the individual under the officer's PACE power.

PNC

- Where an individual has supplied a fingerprint and a match has been found, a PNC Search can be conducted from the CRO number or Immigration details returned.

Retention

Retention of Fingerprint Images Obtained by Mobile Biometrics

- Fingerprints are obtained by attaching a fingerprint reader to a force issue mobile data device.
- The mobile data device has an application installed within its PRONTO operating software which works in a secure environment over a Virtual Private Network (VPN).
- The application captures an image of the individual's fingerprint by placing a finger on the reader, the image is **not** retained on the mobile data device.

- The software sends the image to the source database owned by the home office. Those then return a search result. This is completed against the PNC and Immigration database depending on which options the officer selects.
- Once a result is obtained the fingerprint image cannot be recalled or saved in any way and is deleted.
- Whilst there will be a record of a search being made by the Officer for audit purposes, the initial fingerprint image is **not retained**.

Security

Data

- The fingerprint reader could be lost/stolen in a struggle or other operational circumstances. The reader itself retains no data and is not therefore a security risk.
- The result on the mobile data device is retained and may contain sensitive personal information.
- Mobile data devices are time locked, encrypted and password protected.
- Supervisors will be responsible for conducting checks on their officers to ensure that checks are only being conducted where appropriate grounds exist.

Physical

- The issue of the physical peripheral will be by duty Sergeants at the commencement of duty, they will also ensure they are returned at end of the tour. Sergeants will be responsible for ensuring they are only issued to authorised staff. The software for the search is contained within the officer's mobile data device.
- The fingerprint readers are asset numbered. This means audits can be conducted to verify and account for all devices.
- In the event of loss/theft of a reader, existing reporting protocols **must** be made to Information Security and a Line Manager immediately. A risk assessment and appropriate action will then be taken.

Health & Safety and Training

Health and Safety

- Guidance and West Yorkshire policy will apply to the use of mobile biometrics devices.
- The guidance relates to the care that officers must exercise when using the fingerprint readers, and also the hygiene requirements to clean the device before and after use.
- The cleaning of the device **must** be done before use in the presence of the individual, where possible.

Training

- A simple training package has been produced which will guide officers and staff step by step throughout the biometrics process and remind them of the legal obligations for its use under PACE.
- In addition, officers must have completed the PNC Person E learning, and have been granted access to PNC Persons on their Data Device. This is different to being granted access to desktop PNC, and users are not required to complete a full PNC Desktop Course.
- These packages are mandatory for all device users.
- Once both courses have been successfully completed, access will be granted by the Business Readiness Delivery Team.
- Line managers are to ensure that their staff are using mobile biometrics to its full advantage and that its use is proportionate and legal.

Additional Information

Compliance	This policy complies with the following legislation: • Data Protection Act 2018 • Police and Criminal Evidence Act 1984 • The Mental Capacity Act 2005 • Equality Act 2010 • European Convention on Human Rights (ECHR)
Further Information	Further guidance in relation to this policy can be sought from: • Business Readiness Delivery Team