Home Office

Forensic Information Databases Service (FINDS):

The Forensic Information Databases Strategy Board policy for access and use of DNA samples, DNA profiles, fingerprint images, and associated data

Authorised by: Head of FINDS **Date:** 23rd December 2021

Job Title: Head of FINDS

Shaded areas denote changes from previous version.

Please note that the content and the layout of this document are controlled by the FINDS Quality Team and are not to be altered in any way.

We are constantly looking for ways to improve our policies and procedures. Constructive feedback both positive and negative is always welcome. Please submit your feedback or proposals for change to: FINDS_Quality_Management@homeoffice.pnn.police.uk

Contents

Identification 3
Ownership 3
Distribution 3
Revision History 3
1. Governance 4
2. Objective 4
3. Scope 5
4. References 6
5. Source Materials 7
6. Definitions 8
6. Acronyms and Abbreviations 12
7. Responsibilities 13
8. Overarching Policy 14
8.1. Storage of Data 15
8.2. Policy for Access and Use of DNA Samples and Fingerprint Images 16
8.2.1. DNA 'PACE' samples 17
8.2.2. Fingerprints images 19
8.2.3. Volunteer samples 19
8.2.4. Crime scene samples/images 22
8.2.5. FIND record retention where the subject is deceased before a CPS charging decision 23
8.2.6. Surrogate DNA sample/profile usage 24
8.2.7. Transferring samples or images between Forensic Units, including FSPs 25
8.2.8. National Fingerprint Archive and cross sharing of fingerprint forms between LEAs 25
8.3. Policy for Access and Use of DNA and Fingerprint records 26
8.4. Policy for Access and Use of Associated Data 27
8.5. Control of Access to Forensic Information Databases 28
8.6. Provision of Management Information Derived from the Forensic Information Databases 30
8.7. Use of FIND Data for Research 30
8.8. Records and Audits of Access and Use of FIND Data 31
8.9. Data Protection Impact Assessments for Forensic Information Databases 31
8.10. International Agreements 32
Annex I - Law Enforcement Agencies (LEAs) Permitted Access and Use of DNA Samples, DNA Profiles, Fingerprint Images, and Associated Data 33
Annex II - General Access and Use by specific Forensic information database 34
Annex III - Expanded process, defining stakeholders, data ownership, authority, and lawful purpose 35
Annex IV - FIND Strategy Board Regulation/Oversight model 37
Annex V - IDENT1 Operational and Governance model 37

Identification

Policy Title: The Forensic Information Databases Strategy Board Policy for Access and Use of DNA Samples, DNA Profiles, Fingerprint Images, and Associated Data

Policy Reference Number: FINDS-SB-P-002

Ownership

Department Responsible: FINDS Management

Distribution

FINDS, Forensic Service Providers & Law Enforcement Agencies, FIND Strategy Board and gov.uk website

Revision History

Issue Number	Issue Date	Summary of changes
1	7/6/18	Replaces CUSTP-GP-029 - for expansion to coverage for FINDS
2	21/11/19	DCR403- Rectification of the inaccuracy to the diagram reflecting the MoD purpose for use of BLADE following their feedback
3	23/12/21	DCR300 – Full Document Review

1. Governance

This policy is issued by the Home Office on behalf of the Forensic Information Databases Strategy Board (previously known as the National DNA Database Strategy Board)[1].

The responsibility and accountability for the accuracy and intended meaning of the document resides with the Strategy Board and as such may only be varied or amended with their explicit consent. The governance is set out in the Strategy Board Governance rules which is available from the gov.uk website https://www.gov.uk/government/publications/national-dna-database-strategy-board-governance-rules[2]

2. Objective

The aim is to maintain the integrity of the Forensic Information Databases under the Strategy Board's remit by ensuring that the data is:

- fairly and lawfully retained;
- processed for purposes related to the prevention, investigation, detection, or prosecution of crime, or the execution of criminal penalties, or for the identification of missing people, national security, or prevention of terrorism;
- adequate, but not excessive, for the prevention and detection of crime, and for the identification of missing people;
- accurate and up to date, and held within the appropriate data collection[3] to ensure appropriate use and access;
- retained proportionately; and
- secure.

The principles of the data assurance strategy for the Forensic Information Databases are:

- adherence to quality assurance standards;
- performance monitoring of the end to end supply chain which is supported by the database;
- risk based;
- transparent; and
- supported by an approval process.

[1] Section 63AB of the Police and Criminal Evidence Act 1984 refers to the 'Strategy Board' as the "National DNA Database Strategy Board". The Strategy Board's expanded remit was announced in the Forensic Science Strategy published in 2016; there is no change to the statute.

[2] FIND version is awaiting publication as of December 2021, link is to currently hosted NDNAD (2014) version

[3] Appropriate data collections such as (non-exhaustive) the National DNA Database, Missing Persons DNA Database, Vulnerable Persons DNA Database, and Counter Terrorism (CT) DNA Database

This document describes the specific conditions, permissible purposes, and the level of authority required to access the products of sampling and information derived from Forensic Information Databases including:

- DNA samples and fingerprint images, taken under the Police and Criminal Evidence Act 1984 (PACE) (including all subsequent amendments and variations);
- the Forensic Information Databases retained records where the DNA samples and fingerprint images were taken under corresponding (to PACE) legislation for Scotland, Northern Ireland, and United Kingdom Crown Dependencies;
- the Forensic Information Databases retained records where the DNA samples and fingerprint images were taken under the Terrorism Act 2000, Terrorism Act 2006, Counter-Terrorism Act 2008, Terrorism Prevention and Investigation Measures (TPIM) Act 2011, Counter-Terrorism and Border Security Act 2019, or the corresponding legislation for Scotland, Northern Ireland, and United Kingdom Crown Dependencies;
- Volunteer and crime scene samples and images;
- the results derived from the sampling (including the DNA profile derived from a DNA sample);
- the associated data derived during the processing and searching of data on the Forensic Information Databases; and
- where records are searched against Forensic Information Databases to deliver results, but the searched records are not retained on the database.

The document also specifies the permissible purposes for which the forensic information may be used once accessed.

3. Scope

The policy defines how the Forensic Information Databases meet the principles relating to processing of personal data, as defined in the Part 3 of the Data Protection Act 2018.

This policy applies to:

- DNA samples and fingerprint images taken under PACE, for the detection, investigation, prosecution, and prevention of crime, or the execution of criminal penalties, where the resulting data is intended to be loaded, searched, or compared against the relevant Forensic Information Database – including reference and crime scene samples and images;
- Vulnerable Persons collections on the Vulnerable Persons DNA Database (VPDD) and IDENT1;
- the access to records retained on Forensic Information Databases where the DNA samples and fingerprint images were taken under corresponding (to PACE) legislation for Scotland, Northern Ireland, and United Kingdom Crown Dependencies; and
- the access to records retained on Forensic Information Databases where the DNA samples and fingerprint images were taken under the Terrorism Act 2000, or the Terrorism Act 2006, Counter-Terrorism Act 2008, Terrorism Prevention and Investigation Measures (TPIM) Act 2011, Counter-Terrorism and Border Security Act 2019, or the corresponding legislation for Scotland, Northern Ireland, and United Kingdom Crown Dependencies.

Specific to England and Wales, this policy applies to:

- all DNA samples and corresponding DNA profiles and associated data (collectively referred to as DNA Data), taken in England and Wales for the intended purpose of loading to, searching, or comparing against records held on the National DNA Database (NDNAD) or the Counter Terrorism (CT) DNA Database, or where such DNA Data is utilised in authorised research undertaken to increase the understanding of the impact and/or potential uses of the NDNAD or CT DNA Database; and
- all images of fingerprints and corresponding data (collectively referred to as Fingerprint Data), taken in England and Wales for the intended purpose of loading to, searching or comparing against law enforcement collection records, or the Counter Terrorism (CT) fingerprint collection held on the IDENT1 platform, or where such Fingerprint Data is utilised in authorised research undertaken to increase the understanding of the impact and/or potential uses of Fingerprint Data.

This policy does not cover:

- the legislative provision for the sampling of DNA or fingerprint image;
- the use of DNA or fingerprint data in direct casework comparison;
- access and use of the Missing Persons Databases or Police Elimination Databases (including the DNA Contamination Elimination Database (CED)), as these are covered by separate policies;
- DNA samples or fingerprint images taken in the other UK jurisdictions, for example those taken under Scotland or Northern Ireland legislation, where governance falls to the Scottish Police Authority and the Department of Justice (Northern Ireland) respectively;
- Collections of fingerprint data retained within the IDENT1 platform that are not processed for a law enforcement purpose (unless the collection interfaces with the law enforcement data retained on IDENT1); and
- The interaction and searching between the Immigration and Asylum Biometric System (IABS) and IDENT1, as this is covered by separate policies.

4. References

Title	Reference / Link
Proposal to Conduct Research and Development using Fingerprint and Footwear Images, DNA Samples, Profiles and or NDNAD, IDENT1 or NFD Data	FINDS-F-067
Process for Release from the Forensic Information Databases and the National Footwear Database for Research purposes	FINDS-S-023
International DNA and Fingerprint Exchange Policy for the United Kingdom	FINDS-P-040
FIND Strategy Board Policy and Management of Vulnerable Persons DNA Database (VPDD)	FINDS-SB-P-003
The Control and Avoidance of Contamination in Laboratory Activities involving DNA Evidence Recovery and Analysis	FSR-G-208
Technical Requirements for Processing Samples for National DNA Database Retention/Searching	FINDS-P-031
NPCC Voluntary Attendance National Policy / Guidance v2 (December 2019)	-

5. Source Materials

In preparing the overall policy, due regard has been given to certain legal and policy provisions including, but not limited to, the following (with indicated relevance to specific Forensic Information Database):

	Database relevance	
Legal or policy provision	**NDNAD[4]**	**IDENT1[5]**
Police and Criminal Evidence Act 1984 (PACE) – particularly Part 5	Yes	Yes
Criminal Justice and Public Order Act 1994	Yes	Yes
Criminal Evidence (Amendment) Act 1997	Yes	Yes
Criminal Justice and Police Act 2001 (CJPA)	Yes	Yes
Criminal Justice Act 2003	Yes	Yes
Serious Organised Crime and Police Act 2005	Yes	Yes
Crime and Security Act 2010	Yes	Yes
Protection of Freedoms Act 2012	Yes	Yes
Anti-Social Behaviour, Crime and Policing Act 2014 (ASBC&P) which provides for samples that fall under the Criminal Procedure and Investigations Act 1996 (CPIA) and its associated Code of Practice	Yes	Yes
The Policing and Crime Act 2017 - Section 70 amends PACE to allow retention of DNA profiles and fingerprints taken in England and Wales on the basis of convictions in other jurisdictions, as long as these are for acts which are offences in England and Wales	Yes	Yes
Terrorism Act 2000	Yes	Yes
Terrorism Act 2006	Yes	Yes
Counter-Terrorism Act 2008	Yes	Yes
Terrorism Prevention and Investigation Measures (TPIM) Act 2011	Yes	Yes
Counter-Terrorism and Border Security Act 2019	Yes	Yes
Human Rights Act 1998	Yes	Yes
Data Protection Act 2018 (Part 3)	Yes	Yes
Freedom of Information Act (FOIA) 2000.	Yes	Yes
The Criminal Procedures and Investigations Act 1996 (CPIA)	Yes	Yes
The Forensic Science Regulator's Codes of Practice and Conduct 2021	Yes	Yes
The Accreditation of Forensic Service Providers Regulations 2018	Yes	Yes
Court judgments in particular the Court of Appeal's judgment in X v Z (2015) and X & Anor v Z (Children) & Anor [2015] EWCA Civ 34	Yes	No
Immigration and Asylum Act 1999	No	Yes
Ministry of Defence legal framework	No	Yes

Table 1 Legal or policy provision for Forensic Information Databases

[4] Similarly, applicable to the CT DNA Database

[5] Specifically, the fingerprint collections in IDENT1 used for law enforcement purposes

Home Office Circular	Database relevance	
	NDNAD	IDENT1[6]
16/95 National DNA Database	Yes	No
47/96 Cross search England &Wales with Scotland, Northern Ireland, Channel Islands etc.…	Yes	No
27/97 DNA sampling of prisoners	Yes	No
25/01 Criminal Justice and Police Act 2001	Yes	No
70/02 Retaking of non-intimate samples	Yes	No
20/04 Criminal Justice Act 2003	Yes	No
58/04 Charges on Basis of Speculative Search Match on the National DNA Database	Yes	No
28/05 Serious Organised Crime and Police Act 2005	Yes	No
1/2006: The Application for Access to a DNA Profile for Paternity	Yes	No

Table 2 Home Office circulars for Forensic Information Databases

6. Definitions

Accreditation - third-party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks. In the United Kingdom (UK) the sole national accreditation body recognised by the Government to assess UK organisations that provide certification, testing, inspection, and calibration services is UKAS®.

Associated Data - the information contained on the sampling card, the sampling kits, and any information recorded on the Forensic Information Databases in relation to the records held on the respective database. This information identifies the specific offence for which the sampling event was taken in relation to and/or the individual to whom the DNA sample or fingerprint image and its corresponding data relate.

Contamination - the undesirable introduction of substances or trace materials (for DNA, further detail provided in section 8.2.7).

Controller – means the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by legislation. Where the controller is working collaboratively with other controller(s), they are designated as joint controllers for the purposes of the Data Protection Act 2018.

Competent authority – organisation which is either listed under Schedule 7 of the Data Protection Act 2018 or that has statutory functions for any of the law enforcement purposes[7]; UK police forces, Her Majesty's Revenue and Customs, and the National Crime Agency are listed under Schedule 7.

[6] Specifically, the fingerprint collections in IDENT1 used for law enforcement purposes

[7] The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

CT fingerprint and DNA Databases – Metropolitan Police Service (MPS) Forensic Services is the processor for the CT fingerprint and DNA Databases and is accountable to both the Forensic Information Databases Strategy Board and National Security Biometrics Board (NSBB) for maintaining the integrity of the data held on the CT databases and for ensuring the efficient and effective provision of the database infrastructure, information, and services.

Data Protection Legislation - For the purposes of this document Data Protection Legislation is defined as:

- Retained Regulation (EU) 2016/679 (UK GDPR)[8]; and
- the Data Protection Act 2018 which implements the derogations from the GDPR (EU) (Chapter 2 of Part 2), the GDPR applied to processing outside the scope of EU law (Chapter 3 of Part 2), and transposes (EU) 2016/680 the Law Enforcement Directive (Part 3 of the Act). The vast majority of processing of personal data under this Policy is likely to fall under Part 3.

DNA - Deoxyribonucleic acid, a self-replicating material which is present in nearly all living organisms as the main constituent of chromosomes.

DNA Data – refers jointly to the DNA sample, DNA profile, and Associated Data and is interpreted to also cover any material or information derived or generated from them that would enable an individual to be identified from that data, including any copies of that data.

DNA profile – the genetic interpretation of a DNA sample which is represented on the NDNAD as a series of numbers with a gender marker.

DNA sample – the physical genetic material recovered from a crime scene or provided by an individual.

Fingerprint Data – refers to the fingerprint and palmar images, feature extraction data derived from those images, and associated data that would allow an individual to be identified from that data, including any copies of that data.

Forensic Information Databases Strategy Board - The Strategy Board comprises representatives of the National Police Chiefs' Council, the Home Office, the Biometrics and Forensics Ethics Group, the Association of Police and Crime Commissioners, the Forensic Science Regulator (or representative), the Information Commissioner's Office, the Biometrics Commissioner (or representative), the Scottish Biometrics Commissioner (or representative), representatives from the police and devolved administrations of Scotland and Northern Ireland and such other members who may be invited.

Forensic Service Provider (FSP) - an organisation granted permission by the Forensic Information Databases Strategy Board to provide forensic services to Law Enforcement Agencies (LEAs); in respect of the processing of DNA samples and fingerprint images, and/or the interpretation of the results from that processing, for inclusion in, or comparison against the relevant Forensic Information Database.

[8] The UK GDPR is equivalent to the GDPR with minor amendments, as set out in the Keeling Schedule(s). The schedules cover the GDPR and the Data Protection Act 2018. Some changes include changing references from GDPR to UK GDPR, and the EU regulator to the Information Commissioner's Office.

Forensic Unit - The term 'forensic unit' was coined in the international guidance document (ILAC-G19[9]) on accreditation. It is defined as "*a legal entity or a defined part of a legal entity that performs any part of the forensic science process*".

IDENT1 - is the UK's National Automated Fingerprint Recognition system. IDENT1 comprises the UK National Tenprint Collection (known as the 'Unified Collection'), which consists of fingerprint images obtained from people who have been arrested for a recordable offence within any UK jurisdiction, and unidentified finger marks obtained from scenes of crime (known as the Unidentified Marks Database). IDENT1 also contains collections for Police Elimination fingerprints, fingerprints from Volunteers and Vulnerable persons, and fingerprints relating to Counter Terrorism measures are also stored and searched on IDENT1.

IDENT1 Collections – discrete collections of fingerprint records contained within IDENT1. Collections which have a law enforcement purpose, or interact with a collection that does, are within scope of this policy; this includes the 'SCORD' and 'BLADE' collections in their entirety and those eligible from within the 'Ad Hoc' collection (where discrete containers of fingerprint data can be created for specific purposes).

The Information Commissioner's Office (ICO) - the ICO is the supervisory authority for Forensic Information Databases processing under Part 3 of the Data Protection Act 2018.

International organisation - an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or based on, an agreement between two or more countries.

Law Enforcement Agency (LEA) – any organisation authorised to take samples under PACE.

Management Information - information derived from the Forensic Information Databases to provide high level trend analysis on the composition of the database (e.g. the number and breakdown of records stored, the number of matches between records held for people and crime scene records); and evaluation of profile data to show the effectiveness of the Forensic Information Databases.

National DNA Database (NDNAD) – The NDNAD is comprised of DNA profiles derived from DNA samples taken from crime scenes and DNA profiles derived from DNA samples taken from people who have been arrested for a recordable offence or who have volunteered to have their profile held on the NDNAD; and their Associated Data.

PACE[10] Sample - samples and images taken from all individuals arrested for a recordable offence under PACE where these records are to be retained on the respective Forensic Information Database – NDNAD or IDENT1. It should be noted for DNA samples, the form of the sample comprises of intimate or non-intimate biological samples, such as saliva, blood, plucked/combed hair (head or pubic).

[9] ILAC G19:08/2014 *Modules in a Forensic Science Process*, available at: http://ilac.org/latest_ilac_news/ilac-g19082014-published/

[10] PACE is the relevant legislation for England and Wales. For jurisdictions other than England and Wales their corresponding legislation should be adhered to.

Personal Data - any information relating to an identified or identifiable living individual ('data subject'); an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that individual.

Processor – means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller (other than a person who is an employee of the controller). They must implement appropriate technical and organisational measures that meet the necessary legislative requirements defined in this policy. Processors can be liable for penalties issued by the ICO, or legal claims for damages from data subjects where they have "suffered material or immaterial damage" as a result of an infringement of the processor obligations under the Data Protection Act 2018.

Pseudonymisation - the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Recordable Offence - an offence which must be recorded on the Police National Computer (PNC), and includes:
1. any offence punishable with a term of imprisonment, and

2. a number of non-imprisonable offences have been specified by the Secretary of State (Home Secretary) in regulations as being required to be recorded on the PNC.

Reference (Casework) Sample – DNA samples taken from an individual via PACE but retained under CPIA to support the investigation of a particular case, (or samples taken for elimination purposes (e.g. volunteer and elimination samples). Profiles from volunteer and elimination samples should not be loaded to a national DNA database unless appropriate informed consent has been given by the individual or their legal representative.

(Crime) Scene - a person, vehicle, or location associated with an incident, on or at which may be found evidence to indicate what has happened, when and how, who was involved, and whether a criminal offence may have been committed.

Sensitive Processing – for the purposes of this policy relating specifically to the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual, and the processing of personal data revealing racial or ethnic origin.

Standard Operating Procedure - a written procedure that describes how to perform certain examination or test activities.

Surrogate DNA sample - in a FIND context, a surrogate DNA sample is defined as either Indirect - when DNA is taken from an individual's personal possession or an object that they have come into contact with, or Direct - when DNA is taken from intimate samples from an offender in a criminal investigation, for example penile swabs taken in a sexual assault case.

6. Acronyms and Abbreviations

Short form	Full form	Short form	Full form
ACRO	ACRO Criminal Records Office	**LEA**	Law Enforcement Agency
APCC	The Association of Police and Crime Commissioners	**LED**	Law Enforcement Directive (Directive (EU) 2016/680)
BC	Biometrics Commissioner	**LIMS**	Laboratory Information Management System
BFEG	Biometrics and Forensics Ethics Group	**MoD**	Ministry of Defence
BLADE	Biometric Library of Acquired Exploitation Data	**MoPI**	Management of Police Information
BS	British Standard	**MPU**	UK Missing Persons Unit
CCRC	Criminal Cases Review Commission	**MPDD**	Missing Persons DNA Database
CED	Contamination Elimination Database	**MPS**	Metropolitan Police Service
CJPA	Criminal Justice and Police Act 2001	**NAFIS**	National Automated Fingerprint Identification System
CJS	Criminal Justice System	**NCA**	National Crime Agency
CPIA	Criminal Procedure and Investigations Act 1996	**NCB**	National Central Bureau
CPS	Crown Prosecution Service	**NDES**	National Digital Exploitation Service
CrimPR	Criminal Procedure Rules	**NDNAD**	National DNA Database®
CT	Counter Terrorism	**NI**	Northern Ireland
DNA	Deoxyribonucleic acid	**NPCC**	National Police Chiefs' Council
DPA	Data Protection Act 2018	**NPIRMT**	National Policing Information Risk Management Team
DSTL	Defence Science and Technology Laboratory	**NPPV**	Non-Police Personnel Vetting
DVI	Disaster Victim Identification	**NSBB**	National Security Biometrics Board
DWP	Department of Work and Pensions	**OIC**	Officer in charge
E&W	England and Wales	**ORD**	Operational Response Database
ENFSI	European Network of Forensic Science Institutes	**PACE**	Police and Criminal Evidence Act 1984
FIND	Forensic Information Databases	**PED**	Police Elimination Database
FINDS	Forensic Information Databases Service	**PNC**	Police National Computer
FOIA	Freedom of Information Act	**PoFA**	The Protection of Freedoms Act 2012
FSP	Forensic Service Provider	**PQs**	Parliamentary Questions
FSR	Forensic Science Regulator	**SAR**	Subject Access Request
UK GDPR	Retained Regulation (EU) 2016/679 (UK GDPR)	**SCORD**	Specialist Crime Operational Response Database
GLP	Good Laboratory Practice Regulations 1999	**SFR**	Streamlined Forensic Report
GSC	Government Security Classifications	**SLA**	Service Level Agreement
GSM	Government Security Marking	**SOP**	Standard Operating Procedure
HMGSPF	HMG Security Policy Framework	**SyOps**	Security Operating Procedures
HOB	Home Office Biometric Programme	**T&C**	Terms and Conditions
HOC	Home Office Circular	**TACT**	Terrorism Act 2000
IABS	Immigration and Asylum Biometric System	**TPIM**	Terrorism Prevention and Investigation Measures Act 2011
ICFN	Identity Cards for Foreign Nationals	**UAT**	User acceptance testing
ICO	Information Commissioner's Office	**UKAS**	United Kingdom Accreditation Service
IEC	International Electrotechnical Commission	**UKPPS**	(NCA) UK Protected Persons Service
ILAC	International Laboratory Accreditation Cooperation	**VA**	Voluntary attendee
ISO	International Organisation for Standardisation	**VPDD**	Vulnerable Persons DNA Database

7. Responsibilities

The Chief Officer (or Chief Executive or equivalent) of the Law Enforcement Agency (LEA) where the sampling event took place and the National Police Chiefs' Council (NPCC) Lead for Forensics will be joint controllers in respect of personal data for Forensic Information Databases (FIND) purposes.

It is the responsibility of the FIND Strategy Board to define the policy on how data derived from sampling events taken under PACE powers or volunteer sampling events should be accessed and used. The full responsibilities of the Strategy Board are detailed in *The Governance Rules of the Forensic Information Databases Strategy Board* (originally issued in 2006). https://www.gov.uk/government/publications/national-dna-database-strategy-board-governance-rules[11]

The Forensic Information Databases Service (FINDS) (part of the Home Office) is defined as processor on behalf of the NPCC lead. As defined within the Strategy Board governance rules, FINDS are responsible for the integrity and protection of the data held on the NDNAD and IDENT1[12], and any associated database or collection relating to missing persons, vulnerable persons, or contamination elimination databases.

The Forensic Science Regulator is appointed by the Home Secretary to be responsible for the setting of, and compliance with, national quality standards for the provision of forensic science services to the Criminal Justice System in the United Kingdom, including, but not limited to, those relating to the National DNA and Fingerprint Databases.

The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Information Commissioner will help to ensure that the Board gives due weight to the demands of the Data Protection Act and other privacy legislation to ensure that the Forensic Information Databases retain the confidence of all communities. The ICO is the supervisory authority in relation to this processing under Part 3 of the Data Protection Act 2018.

The Biometrics Commissioner is independent of government. Their role is to keep under review the retention and use by the police of DNA samples, DNA profiles, and fingerprints.

LEAs are responsible for ensuring the continuity of evidence for each sample they have taken and will be responsible, through their Data Protection Officer function to report breaches of privacy to the ICO.

Forensic Units are responsible for assuring that they comply to legislative, regulative, and policy requirements to ensure the integrity of the records held on the Forensic Information Databases; where the database is not directly under FINDS management, there is a need for Units to establish dialogue with FINDS to ensure consistent adoption of this policy.

Commercial Forensic Service Providers (FSPs) are processors on behalf of the LEA where the sample was taken and will process according to the instructions of the LEA with the appropriate contractual arrangements.

[11] FIND version is awaiting publication as of December 2021, link is to currently hosted NDNAD (2014) version

[12] Specifically, the fingerprint collections in IDENT1 used for law enforcement purposes

All organisations which actively undertake sensitive processing must adhere to the requirements of data protection legislation to include that stated in the Data Protection Act 2018.

It is the responsibility of LEAs, FSPs, and any other agency or organisation acting on their behalf to comply with this policy. If there is any doubt as to whether a specific action or activity complies with this policy, then clarification should be sought from the Forensic Information Databases Strategy Board (through the FINDS) prior to commencement.

8. Overarching Policy

The Chief Officer (or equivalent) of the LEA who determines the purposes and means of the processing of personal data by performing the sampling event is the controller for all data linked to that DNA sample or fingerprint image.

DNA and Fingerprint Data may not be used directly or provided to any other agency or organisation for purposes other than those listed in Annex I or those specifically authorised by the Strategy Board.

Forensic Units submitting information to the Forensic Information Databases must be accredited to the international standard ISO17025 and the Forensic Science Regulator's Codes of Practice and Conduct where these are currently applicable, or otherwise must be meeting the minimum requirements of the respective database system.

Specific to the DNA, where commercial FSPs support the process for generation of PACE DNA profile records for NDNAD purposes, the identity of a known individual must not be provided to the FSP unless the allowance is given within this policy.

In the case of processing DNA Samples, it is mandatory that the Forensic Unit (including FSPs) using logging systems (for example a Laboratory Information Management System (LIMS)) do not solely retain the sample barcode present on the PACE or CJ sampling kits but instead also assign a unique processing identifier to the subject's DNA Sample; this action enables the profiling record to be de-linked from the barcode to adhere to legislation (i.e. on deletion of the corresponding DNA profile record retained on the NDNAD).This is optional for samples taken with volunteer sampling kits. It should be noted that Forensic Units will hold details of volunteer and elimination samples as the databases do not receive this information from the Police National Computer (PNC).

IT support for Forensic Information Databases

For the purposes of provision of IT support for the Forensic Information Databases, the service provider must ensure that all supported environments, for example, any Test and Development instances, comply with this policy and legislative requirements (including the retention regime) specified within this policy. Where the database system setup is such that datasets can be linked through the live environment for functionality test and development, or for validation purposes, the same requirements are applicable.

Where the supported environments/datasets contain fields within which personal data is populated, this data must be anonymised as a minimum. There must be full transparency for the environments and datasets retained in order that the Strategy Board, administered by FINDS on their behalf, have the necessary oversight to be able to track the purpose, authority and approvals in place, and afford the same level of scrutiny to all regardless of the system container.

A general principle in order for the environment to comply with legislative requirements, such as PACE as amended by the Protection of Freedoms Act (2012) (PoFA), is that where there has been deletion of a record from a Forensic Information Database, this should be migrated to all supported environments through record deletion or removal of any linkage between the record retained and all those demographic fields that can be used to uniquely identify individuals such that it is not possible to subsequently attribute the record to a specific individual. This aligns to the fifth data protection principle as data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

There is requirement for the National DNA Database to be conforming to the Forensic Science Regulator 'Codes of Practice and Conduct', with the independent assurance mechanisms used to ensure that the standards have been met being ISO 9001, and ISO 27000 and the 20000 series (as provided through the TickIT*plus* scheme) for the supporting IT infrastructure and service management functions respectively.

8.1. Storage of Data

For Government Security Classifications (GSC) purposes, the FIND have the status of 'Official Sensitive' with there being appropriate handling instruction added to the generated documents.

DNA and Fingerprint Data, including law enforcement data retained on the NDNAD and IDENT1 and related records held by the Forensic Units and LEAs, must be managed in accordance with Data Protection Principles. Retention of these records must comply with legislative requirements and the accuracy of the records must be maintained.

Considering Data Protection, there must be allowance for controllers (through processors, as necessary) to:

- Implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing, to meet the requirements of the Data Protection Act 2018 (Part 3) and protect the rights of data subjects.
- By default, ensure that only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. It is advisable that the lawful basis for processing the data is logged and recorded.
- Assess the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with Data Protection Act 2018 (Part 3), taking into account the rights and legitimate interests of the data subjects and other persons concerned. This point is specifically pertinent for implementing new technologies, mechanisms or procedures which involve a high risk to the rights and freedoms of data subjects (identified through data protection/privacy impact assessment) and measures to reduce that risk have not been fully defined – in these the controller or processor must consult the supervisory authority (in this case, the ICO) prior to processing.

IT system providers for the Forensic Information Databases should be working to the principles of the ISO/IEC 27000 standard (as provided through the TickIT*plus* scheme) in order that key Data Protection Act 2018 (Part 3) controls are in place (such as auditing of system access and data changes).

The FINDS Unit defines the processes to meet their obligations through the following documentation and procedures:

Documentation	Database relevance	
	NDNAD	IDENT[13]
FINDS-P-028 - Performance Requirements and Monitoring of Suppliers of Profiles to the National DNA Database	Yes	No
FINDS-P-024 - ACRO Record Deletion Process Procedure for the Deletion and Destruction of DNA Records and Samples	Yes	Yes
FINDS-P-037 - Procedure for the Deletion and/or Destruction of DNA Samples and Records	Yes	Yes
FINDS-SB-P-001 - Forensic Information Databases Strategy Board: Guidance to Ensure Matches are Lawful - Protection of Freedoms Act	Yes	Yes
NDNAD RMADS – Security Operating Procedures	Yes	No
IDENT1 Security Operating Procedures (SyOps)	No	Yes
Forensic Science Regulator's Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System	Yes	Yes
ISO/IEC 27000-series of standards - Information technology - Security techniques - Information security management systems (as provided through the TickIT*plus* scheme): • ISO/IEC 27000:2016 - Overview and vocabulary. • ISO/IEC 27001:2013 – Requirements. • ISO/IEC 27002:2013 - Code of practice for information security controls. • ISO/IEC 27017:2015 – Cloud security • ISO/IEC 27018:2019 – Cloud data protection	Yes	Yes
ISO/IEC 20000 standard for IT service management (as provided through the TickIT*plus* scheme): • 20000-1: Service management system requirements • 20000-2: Guidance on the application of service management systems • 20000-3: Service providers • 20000-4: Process assessment model • 20000-5: Exemplar implementation plan for ISO/IEC 20000-1 • 20000-9: Guidance on the application of ISO/IEC 20000-1 to cloud services • 20000-10: Concepts and terminology • 20000-11: Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: ITIL®	Yes	Yes

Table 3 Documentation for Forensic Information Databases system management

8.2. Policy for Access and Use of DNA Samples and Fingerprint Images

Once obtained, DNA samples and fingerprint images may only be accessed by LEA staff, or parties working on behalf of a LEA (including for the purposes of the international sharing of data). The LEA controller may define specific contractual constraints regarding the access to DNA Samples or fingerprint images on any third party (e.g. FSP or a different Forensic Unit within LEA) acting on their behalf.

On receipt of a DNA sample or fingerprint image, the Forensic Unit may only access that sample or image to:

[13] Specifically, the fingerprint collections in IDENT1 used for law enforcement purposes

- derive the result for the purpose of loading to, searching against or comparing against existing results held on the Forensic Information Database or other results specific to the case under investigation (in the case of DNA, this will include an extract of a previously processed DNA sample, where permission has been granted by the Chair of the FIND Strategy Board); or to
- destroy the DNA sample or fingerprint image.

In the case of retained subject DNA, samples may be accessed and profiled:

- where no profile has been obtained from the initial analysis of a sample;
- for alternative analysis (e.g. Y-STR or paternity analysis) if this analysis relates to the investigation of the case for which the sample has been taken and the sample is held under CPIA by the FSP (the FSP should be notified by the owning force at the point of submission - or as soon as possible after, acknowledging section 8.2.1a - in writing (electronically) if the sample is to be held under CPIA); or
- to comply with the quality assurance programme as set by FINDS. This should include any reprocessing of a DNA sample where it is required to establish the accuracy of the DNA profile(s) obtained.

8.2.1. DNA 'PACE' samples

To conform to PACE as amended by the Protection of Freedoms Act (2012) (PoFA) requirement, DNA samples must be destroyed as soon as a DNA profile has been satisfactorily derived from the sample (including the carrying out of the necessary quality and integrity checks) and, in any event, within six months of the taking of the sample.

Where a sample is processed and a profile generated for NDNAD search/retention purposes, but the profile is not submitted within 6 months of the DNA sample being taken, there is a need to ensure that for any subsequent submission (i.e. after 6 months of the DNA sample being taken) that there is confirmation from the owning Force that they wish for the profile to be submitted to the NDNAD and can confirm that there is a power under PACE as amended by PoFA for this to occur.

a) CPIA retention

There may be some circumstances where a PACE sample is required to be retained because challenges may be raised in court proceedings which would require it to be analysed and this could not be done if it has been destroyed. This would involve casework – i.e. expert analysis of the sample by a forensic scientist or scientists. This is regulated through CPIA.
If an LEA has an operational need to retain a PACE sample under CPIA for casework, the Forensic Unit must be notified at the time of submitting the sample for analysis, or as soon as possible after submission. If requests are made after the sample has been submitted, there is a risk that it may have already been destroyed under PoFA requirements; without CPIA retention, from the date of Forensic Unit receipt of a sample, there is a **maximum** allowable timespan of 16 weeks before the sample destruction activities must have been completed, further details for this aspect are contained within document FINDS-P-028 'Performance Requirements and Monitoring of Suppliers of Profiles to the National DNA Database'.

The request for retention must be made in writing (electronically) and must include:

- barcode,

- explicitly state that the sample is to be retained by CPIA,
- the name of the person requesting retention, and
- case number (if possible).

It should be noted that the decision to retain must consider the appropriateness of the retention and data minimisation principle defined within CPIA, and LEAs must evidence the necessity of the retention, with the underlying principle being that this must be performed on a case by case basis rather than, for example, simply due to the type of offence. The numbers of samples or images being retained under CPIA will be monitored by the FIND Strategy Board and, along with the reason for retention, is of interest to the Biometrics Commissioner's Office[14]. In order to ensure that the retention of samples under CPIA is lawful and proportionate the onus is on LEAs to review PACE DNA samples held under CPIA every three months and inform the FSP when it is appropriate to destroy.

For a sample retained under CPIA, the six-month destruction provision as part of PoFA no longer applies, however any such sample can only be used for proceedings for the offence in connection with which it was taken and must be destroyed once no longer required for any proceedings or appeal relating to that offence. Samples retained under CPIA may be subject to profiling or alternative analysis even after six months. Profiles derived from these samples after six months can be used only in relation to the offence in connection with which they were taken. To explain this, two examples are given:

Example 1: a sample is taken and profile #1 obtained and loaded to the NDNAD within six months. The sample is retained beyond six months under CPIA and alternative analysis carried out. Profile #1 can be retained on the NDNAD for general searching (under section 63E of PACE which permits retention if there is an ongoing investigation, or any other relevant section) as the provision relating to CPIA does not apply to it, as it was generated within the six-month period. But any searching using the results of the alternative analysis must be limited to that related to the offence for which the DNA was taken.

Example 2: a sample is taken, and no profiling carried out. The sample is retained beyond six months under CPIA. A profile is then derived. This profile is governed by the provision relating to CPIA and so can only be used in relation to the offence for which it was taken, not for general (NDNAD) searching.

LEAs should also ensure that the need to retain any PACE sample which they hold 'in LEA' is reviewed at least every three months and that such samples are promptly destroyed unless there is good reason for them to be retained.

b) General usage considerations for samples retained under CPIA

Section 63R of PACE as amended by PoFA states that DNA samples taken by the police (either with or without consent) must be destroyed as soon as a DNA profile has been satisfactorily derived from the sample (including the carrying out of the necessary quality and integrity checks) and, in any event, within six months of the taking of the sample. However, section 63U states the destruction requirement in section 63R does not apply if the sample is or may become disclosable under CPIA or the CPIA Code of Practice. It goes on to state that a sample preserved under CPIA retention can only be used in relation to the offence for which the sample was taken and must be destroyed once CPIA retention ceases to apply.

[14] As mentioned in 'Annual Report 2020, Commissioner for the Retention and Use of Biometric Material', section 60

Where a PACE sample is received by a Forensic Unit where there is notification on the submission paperwork from the police force that the PACE sample is 'CPIA retained', the PACE status of the sample allows submission of a generated DNA-17/DNA-20+ profile to the NDNAD as well as any alternative testing that may occur through the allowance of the CPIA retention aspect. It is of note that the generation of the DNA-17/DNA-20+ profile may post-date that of a profile generated through alternative testing, and that this specific element does not impact upon the ability to submit the DNA-17/DNA-20+ profile for NDNAD search/retention – PACE is in place for NDNAD purposes, and CPIA is in place for casework usage of a profile generated through alternative testing.

For sample destruction purposes, the CPIA retention aspect is implicit in the destruction requirements such that:

- for example, where a DNA PACE sample is initially submitted with CPIA retention and subject to Y-STR profiling and then subsequently profiled for NDNAD purposes, if the sample remains under CPIA retention, then destruction does not occur (until the point at which the CPIA retention is removed), and
- where a DNA PACE sample is initially submitted with CPIA retention and subject to Y-STR profiling, following which the CPIA retention is then removed, there remains the allowance for the sample to be profiled for NDNAD purposes (with the standard DNA PACE sample destruction requirements as detailed in section 8.2.1 paragraph 1).

c) CPIA retention invalidated by NDNAD profile deletion

For PACE samples retained under CPIA for which the representative DNA profile record has been deleted from the NDNAD, on FSP receipt of the deletion (de-linking) message from the FINDS NDNAD team, there must be destruction of the physical DNA sample.

8.2.2. Fingerprints images

For fingerprints purposes, the retention of fingerprint forms is clearly defined under PACE (as amended by the Protection of Freedoms Act 2012) that any fingerprints that no longer meet the retention criteria under PACE must be destroyed. These include original hardcopy forms; electronic images; and any copies thereof.

However, in certain circumstances under CPIA it is not only permissible, but advisable to store fingerprints within a casefile; even though retention under PACE is no longer lawful. This is to ensure that any person reviewing the case at a later date, either as part of a prosecution or a cold case review has access to the relevant materials. Any fingerprints stored for this purpose must only be used for the case for which they are stored; and cannot be used in conjunction with any other unrelated investigation. There should not be any signposting to the existence of these forms from any electronic or manual database (including the local fingerprint collections), to mitigate the risk that they are used inappropriately.

8.2.3. Volunteer samples

Elimination Sample/Images

The sample destruction requirements for a sample which has been taken with consent and in connection with the investigation of an offence (an 'elimination sample') should align to PACE as amended by the Protection of Freedoms Act (2012) as defined in section 8.2.1.

Elimination samples may include those taken from someone who is suspected of having been the victim of a criminal offence; from partners and relatives of the suspected victim; or as part of a mass screening exercise. Any such sample must only be used for the purposes of the offence and/or enquiry in connection with which it was taken and for which consent was given and must only be retained beyond 6 months in exceptional circumstances where CPIA applies.

If an LEA has an operational need to retain an elimination sample under CPIA for casework, the process defined in section 8.2.1a is to be followed. The onus is on LEAs to review any elimination samples held under CPIA every three months and inform the FSP when its retention ceases to be necessary it is appropriate to destroy. LEAs should also ensure that the need to retain any elimination sample which they hold 'in LEA' is reviewed at least every three months and that such samples are promptly destroyed unless there is good reason for them to be retained.

For fingerprints purposes, where a local Operational Response Database (ORD) is constructed which includes records where the images were taken under PACE for elimination purposes, the usage of such records can only be in the specific case that they were taken for, and there must be consent gained from the individual sampled for the retention. All additional records held within an ORD must comply the relevant retention legislation or consent obtained for the sampling, with the owner of the ORD being responsible for the appropriate management of data contained within.

Other Volunteer Samples/Images

For DNA samples and fingerprint images which are taken with informed consent, but not in connection with the investigation of an offence, such as DNA samples taken from vulnerable volunteers or from relatives of missing persons (who are not suspected to be the victims of offences), there is no legal requirement for destruction. This is because section 63R(1)(b) of PACE states that the sample destruction provisions apply to samples 'taken by the police, with the consent of the person from whom they were taken, in connection with the investigation of an offence by the police' – i.e. if there is no investigation of an offence the sample destruction provisions do not apply. Examples are provided below:

- Vulnerable volunteers

  If a vulnerable person (e.g. a potential victim of honour-based assault) gives consent for their DNA sample or fingerprints image to be taken, the sample/image is not required to be destroyed within any specific period if no offence is suspected to have taken place at the time of the sample/image being provided. However, the retention of the sample/image must be reviewed by the LEA every 2 years and must be destroyed if it becomes apparent that there is no good reason for them to be retained (it is responsibility of the LEA to request the destruction from the FSP).

- Missing persons

  Where an individual has been reported missing, a relative of the individual may agree to consent to provide a DNA sample in case their relative's body is discovered at a later date. In such cases, the DNA sample can be retained until any investigation into the missing person has concluded.

This retention may be beyond the life of the relative so as to allow for identification years after the person went missing. Due to the potential degradation that may occur over time to non-located bodies, alternative DNA tests (on both the body and relative sample for comparison) may be required. For sample destruction, it is responsibility of the LEA to request the destruction from the FSP.

Volunteer samples/images and the associated data must be destroyed when either:

- (missing person related) identification is made and the case is concluded,
- the consent for retention has been removed,
- when the vulnerable person is assessed as no longer being vulnerable, or
- on request from the volunteer

In addition, in cases where DNA samples are taken from the missing persons personal belongings such as a toothbrush, these are considered to be in-direct reference samples and are also not required to be destroyed.

Volunteer samples - consent aspect where counter/signature is not available

In cases where the donor of the DNA sample is physically unable to provide their consent by signature on the DNA Elimination Kit Form, and a countersignature is not available, for example:

- samples taken from babies in cases such as abandonment, where a parent or guardian is not available to sign on their behalf, or
- a victim is DNA sampled where the victim has injuries which hamper their ability to be able to sign, and for which other family members are not available;

it is acceptable for a member of the Police Force undertaking the DNA sampling to sign on the DNA sample donor's behalf. On submission of the DNA kit to their FSP for processing, Forces should ensure to provide the reasoning behind the lack of signature in order that the FSP can process the sample without any delay i.e. whilst querying this with the Force. The same consent allowance is given to the taking of fingerprints respectively.

With particular relevance to vulnerable volunteers, in cases where consent was originally given for the DNA sampling, but the Force are seeking a fresh signature, for example where a replacement sampling form is necessary (but the overall purpose and usage of the sample and generated DNA profile is consistent), there are scenarios where contacting the volunteer donor for these purposes may not be feasible/appropriate. Where a Force assessment concludes that contacting the donor would put them at some risk of harm, or the donor is no longer resident in the UK and cannot be located, it is acceptable for a member of the Police Force to sign on the donor's behalf.

In cases where the donor of the DNA sample is a young person, under the age of 16, who has been the victim of a serious and/or sexual crime and attended a Sexual Assault Referral Centre (SARC) without a responsible adult; the principles of the young person being Gillick competent to consent to have an elimination sample taken, and therefore not requiring a countersignature, should be employed.

Where the donor of the DNA sample is a young person of age 16 or 17, there is the ability for the young person to self-consent to have an elimination sample taken, and therefore there is not a requirement for a countersignature. Clarification on the Gillick Competency/Fraser Guidelines is present in detail within document FINDS-SB-P-003 'FIND Strategy Board Policy and Management of Vulnerable Persons DNA Database (VPDD).

FSPs in receipt of volunteer samples where the corresponding paperwork does not include the countersignature should not reject the sample for processing purely on the basis of lack of countersignature; if there is information available from Force that confers the appropriate status for the sample, then processing is able to take place.

In these cases, the usage of the sample, generated records, and associated data is identical to if the volunteer had been able to sign.

Voluntary Attendees

A Voluntary attendee (VA) is an individual who is suspected of committing an offence and who is willing to cooperate with the police investigation without being arrested and where they attend a police station/agreed venue for interview and processing which is carried out in accordance with PACE.

The NPCC Voluntary Attendance National Policy / Guidance v2 (December 2019) states that fingerprints and DNA should not be taken voluntarily at VA Interview, and that instead the sampling of fingerprints and DNA is required when the individual is either charged, cautioned, or reported for the offence(s).

For Forensic Information Databases purposes, the controller is responsible to ensure that full instruction is given to the processor to enable only those DNA and fingerprints records with the appropriate legal authority are submitted for NDNAD and IDENT1 retention respectively.

8.2.4. Crime scene samples/images

Records should be loaded to Forensic Information Databases that are appropriate e.g. in-line with this policy and measures to prevent unwittingly loading a record that does not relate to the offender should be taken. Elimination samples/images should be obtained from those with legitimate access to the crime scene as appropriate in the particular case. However, if the provision of an elimination sample/image is not possible it is permissible to load any record obtained from a scene of crime where it is believed to be related to that crime and has evidential value. The LEA should be aware of the risks of this approach with court disclosure of previous offences, should a crime scene profile prove to match a victim.

As a rule, there should be only one copy of a particular crime scene record held per case reference on a Forensic Information Database; duplicate loads should be avoided. Subsequently after loading, should a record be found that belongs to a victim, is considered not to be related to the crime, or is no longer relevant to the investigation then the sampling LEA must ensure that the record is deleted from the Forensic Information Database as soon as possible. In these circumstances, the release of the victim's record from the Forensic Information Database will not be automatically forthcoming without the specific, informed consent of the victim (including in the case of an NDNAD match).[15]

[15] This policy should not impact the ability of FSPs to respond to urgent requests and as such crime scene records can be retrospectively loaded to NDNAD by FSPs following a direct comparison as discussed through the particular case forensic strategy or more generally through their LEA Service Level Agreements.

Records from detected crimes (e.g. for DNA where there is a significant NDNAD match identified from full SGMPlus or DNA-17 profiles) should be removed from the Forensic Information Database as soon as practicable by the LEA requesting FINDS to perform such a deletion (where appropriate).

8.2.5. FIND record retention where the subject is deceased before a CPS charging decision

The 'Deceased Suspects - CPS Policy on Charging Decisions' guidance[16] describes that since deceased persons cannot be prosecuted, the CPS will not make a charging decision in respect of a suspect who is deceased. This applies in all cases where the suspect is deceased, including cases in which the police made a referral to the CPS for a charging decision prior to the suspect's death. Further detail is provided for the scenario where a suspect may die during an investigation, after the police have referred a case to the CPS, but before the case has been fully reviewed and a charging decision made. In these cases, the police may decide whether any further investigative steps should be taken and whether they wish to state publicly their view on the sufficiency of evidence.

FIND record retention - decision process

For the purposes of suitability of the submission of a record for FIND retention in cases where the suspect dies before proceedings could be initiated or completed:

1. The offence(s) attributed to the suspect must be of 'Serious' status (examples from the NDNAD classification include murder, rape, and terrorism related offences), where the investigating force have determined that there is potential for a serial nature (or otherwise further offences as to yet undiscovered) of offending such that there is an increased likelihood of crime scenes being discovered in the future.
2. Forces must ensure that there is approval for the FIND retention from the senior investigating officer (or equivalent) for the case.
3. The supporting documentation or case papers must contain sufficient evidence to charge had the offender not have died before proceedings could be initiated or completed. Forces may also register a Recorded Crime Outcome, if in their view there was sufficient evidence to charge the suspect, if the suspect were still alive.

Ethical considerations

Where there is a linkage between an unsolved offence and deceased subject through a match generated on a FIND, there should be acknowledgment of the potential impact to the reputations of the deceased subject and their families of the release of this information into the public domain. On that basis, if there is to be the attribution of an offence to the deceased subject, the investigation must follow the standard pathway and (as 3 above) conclude with sufficient evidence to charge had the offender not died before proceedings could be initiated or completed, with the potential to also register a Recorded Crime Outcome, if in the view of the investigating Force there was sufficient evidence to charge the suspect, if the suspect were still alive.

[16] https://www.cps.gov.uk/legal-guidance/deceased-suspects-cps-policy-charging-decisions

8.2.6. Surrogate DNA sample/profile usage[17]

In a FIND context, a surrogate DNA sample is defined as:

- Indirect: is the term used when DNA is taken from an individual's personal possession, such as a toothbrush, razor, or even an object that they have come into contact with;

- Direct: is the term used when DNA is taken from intimate samples, from an offender in a criminal investigation, for example penile swabs taken in a sexual assault case. In such an example, the penile swabs are used for the purpose they were intended (crime stain) and/or being used as a reference DNA sample in the absence of a PACE sample being retained under the Criminal Procedures and Investigations Act 1996 (CPIA).

To note that this guidance is not applicable in relation to surrogate DNA samples/profiles used specifically in missing persons cases, for which document FINDS-P-019 'Policy for administering the Missing Persons DNA Database for the National Crime Agency - UK Missing Persons Unit' contains the relevant information.

A surrogate DNA sample should only be used as a last resort in criminal investigations, where a PACE DNA sample is not possible or where the individual refuses to provide an elimination DNA sample to assist.

For the purposes of legislation, the relevant police powers for surrogate DNA samples are the general powers of seizure and retention found in sections 19 and 22 of PACE (in Part II). Taking the provisions of Part II of PACE together with the authority of *X & Anor v Z (Children) & Anor* [2015] EWCA Civ 34, the advice is that there are clear statutory powers for the seizure and retention of surrogate DNA samples – provided the criteria set out in sections 19 and 22 of PACE have been met. It is the responsibility of the owning Law Enforcement Agency (LEA) to determine that the above provisions of PACE have been met, before requesting a FSP to undertake this kind of work.

DNA sample retention - where the criteria set out in sections 19 and 22 of PACE have been met, and a surrogate DNA sample has been taken, then the DNA sample must be destroyed as soon as a DNA profile has been satisfactorily derived from the sample (including the carrying out of the necessary quality and integrity checks) and, in any event, within six months of taking the sample; alternatively, a request for CPIA retention should be made.

DNA profile - NDNAD searching - surrogate reference DNA profiles are permitted to be speculatively searched against the NDNAD; however, the permanent retention of these DNA profiles is not permitted (with there not being a mechanism in place to drive a specific retention period or deletion for such records).

[17] This is not applicable to crime stain samples/profiles, considering the scenario with the sample as a vaginal swab in a rape, and the victim being necessarily part of the crime scene, where a mixture profile is generated but no elimination sample is available from the victim, the victim portion of the mixture does not constitute a surrogate status as was developed from crime scene material.

8.2.7. Transferring samples or images between Forensic Units, including FSPs

In instances where physical DNA samples or fingerprint images, for example the second swab from a PACE sampling kit, (subject to retention limits) are transferred between Forensic Units, including FSPs, the submitting Forensic Unit must supply all the remaining sample, the original DNA form/LEA submission documentation (which must include the date sample taken) and documented evidence of a CPIA exemption instruction (if appropriate) to the receiving FSP. The FSP receiving the sample is responsible for the subsequent control/retention and eventual destruction of the received material. These transfers occur outside of the Forensic Information Database domain.

There are no restrictions on the transfer of crime scene material other than normal measures to retain continuity and any other requirements defined by the controller.

Document reference FINDS-P-031 'Technical Requirements for Processing Samples for National DNA Database Retention/Searching' section 9 'Processing of samples from other FSPs' describes the requirements in detail for DNA sample transfer, acknowledging the risk for contamination. For the purposes of this policy, contamination is defined as stated in the FSR-G-208 'The Control and Avoidance of Contamination in Laboratory Activities involving DNA Evidence Recovery and Analysis' as "*the introduction of DNA, or biological material containing DNA, to an exhibit or subsample derived from an exhibit at or after the point when a controlled forensic process starts". This is distinct from the adventitious transfer of biological material to an exhibit that can also occur, usually prior to the exhibit or sample being recovered and before investigative agencies have intervened*"; with the definition for unsourced contaminant being '*A DNA profile identified as a contaminant, i.e. following all relevant elimination database checks of which the source has not been identified. No template (negative) controls and quality control batch tests are considered as having originated from the manufacturing supply chain, historically most have been found to come from manufacturing staff'.*

For fingerprint purposes, any LEA which accesses and retains - e.g. printouts of a fingerprint record - is responsible for any subsequent destruction as required by PACE as amended by PoFA (or else otherwise covered within CPIA retention).

8.2.8. National Fingerprint Archive and cross sharing of fingerprint forms between LEAs

Historical fingerprint forms dating from the introduction of the fingerprint system in the UK to the point where the National Automated Fingerprint Identification System (NAFIS) was fully implemented, are held at the National Fingerprint Archive:

- these are derived from all police jurisdictions in England & Wales, as well as copies of fingerprint forms obtained by Police Scotland;
- they are stored and maintained in relation to current retention legislation;
- requests can be made by LEAs to retrieve copies of these fingerprints so that they can be used locally to identify individuals, or compared against casework;
- similarly, each LEA has the ability to share copies of fingerprint forms between each other in the knowledge of their retention responsibilities under PACE, Management of Police Information (MoPI), and CPIA; and

- the sharing of forms, either postal or electronic, must be done using approved security protocols.

8.3. Policy for Access and Use of DNA and Fingerprint records

The DNA and fingerprint data collections will be the primary reference point for gaining PACE sample data.

For DNA, any request to release any profile that is held on the NDNAD must be made through the FINDS. Exceptions will be made:

- whereby Forensic Units will be able to release records out of the FINDS normal office hours[18], or
- where additional DNA profile markers/values are available for an NDNAD retained profile record (where the additional markers/values are not currently able to be retained by the NDNAD).

The LEA must inform the FSP that the profile being sought is legally held at the point the request to release is made.

DNA and fingerprint records[19] must only be used for:

- the provision of intelligence and evidence to support the investigation, detection, prosecution, and reduction of crime and in the interests of national security as defined in s.63T of PACE;
- the identification of a deceased person or of the person from whom a body part came;
- the protection of an individual who has volunteered their sample as they are potentially at risk of harm;
- Counter Terrorism purposes; or
- Immigration Enforcement.

This may take the form of:

- Conducting searches against the records held on the respective database.
- Comparison against a specific case including conducting eliminations of matches (under CPIA).
- Comparison against specific records held on the respective databases.
- Performing quality checks in relation to the processing of DNA samples and fingerprint information as limited by section 8.2.

[18] (Mon-Friday 08:00 to 18:00 and weekend days from 09:00 to 12:00)

[19] This will primarily relate to the use of the offender's DNA and not the victim's. Profile release of the victim would only occur in exceptional circumstances through authorisation by the Chair (or nominee) of the FIND Strategy Board, even where a match report has been generated from the NDNAD; for such approved releases, the necessary Force legal agreement to progress with the case on the basis of the profile release would also need to be in place.

- In exceptional cases, where the requirement of the case is not otherwise described in this policy or a specific legally based agreement for retention, gaining Strategy Board approval should a record require permanent loading to the NDNAD that does not meet the criteria defined in this policy.
- In order to use a DNA sample and/or profile for the purposes of criminal paternity investigations, a PACE sample must be collected wherever possible for the offence under investigation. The subject must be informed that the sample and/or profile may be used for paternity analysis. Profiles from PACE samples must only be sought where the profile will assist the investigation; for example, in a criminal paternity investigation, if the suspect has denied contact with the complainant, DNA would assist in supporting (or opposing) this proposition. If the suspect admits intercourse but maintains it was consensual, DNA cannot address this proposition. The profile in this second example would need a deeper review to determine if the profile could be used under PACE: if required, a casework reference sample should then be sought. See also Home Office Circular 1/2006 "The application for access to a DNA profile for paternity".

The Court of Appeal judgment in X v Z (2015) found that biometrics collected under the evidence gathering powers of Part 2 of PACE may be retained and used only for the purposes of criminal law enforcement function. Thus, such data cannot be used, for example, in order to resolve issues of paternity in care proceedings before the family court.

Considering the interaction between the MOD special collection and IDENT1 detailed within 'Annex V - IDENT1 Operational and Governance model' of this document, this interaction being one of processing anonymised fingerprint records rather than actually accessing the fingerprint collection itself negates the specific need for the presence of a legal authority (either in statute or at common law); however any subsequent processing of sensitive personal data of an identifiable individual, by either a police force or the MOD, must be in accordance with the relevant data protection legislation.

8.4. Policy for Access and Use of Associated Data

The data associated with DNA samples and fingerprint images and their corresponding profiles and records must only be used to:

- Evaluate the result from a search performed against the respective database.
- Confirm the integrity of the records held on the Forensic Information Databases.
- Restrict the search parameters of a non-routine speculative search of the NDNAD
- For subject samples only - identify a sample or profile when being transferred between FSPs for DNA profile comparisons where there is a link to an individual. For DNA, best practice is to use two separate identifiers; usually the sample identifier barcode and one other identifier e.g. date of birth.

Controllers and processors must ensure any transfer of subject records complies with legislative requirements. No transfer of data from records deleted from the Forensic Information Databases is permitted. Any data originally transferred from a subsequently deleted record must also be deleted, except for those records transferred to the Missing Persons databases for DNA and fingerprints, where they are retained under CPIA.

Although it is legitimate for the Forensic Information Database to have full or partial automation for database activities, the use of outputs (for example, the Police Force being in receipt of a NDNAD Match Report) from the database must prohibit generation of a decision based solely on automated processing; this being to ensure appropriate safeguards are in place for the rights and freedoms of a data subject, with at least the right to not to be subject to a decision based solely on automated decision making.

For any services delivered from a Forensic Information Database where there is use of personal data, such as self-determined ethnic origin, to process a database search, the requirement is that this occurs where authorised by the source legislation (that the sample was taken under) or to protect the vital interests of the data subject or of another natural person.

For Forensic Information Databases, rectification of inaccurate personal data may be automated through linkage with systems where records are administered by the controller, for example personal data amendments on the Police National Computer (PNC) migrate to the NDNAD and IDENT1 (where the relevant field is present). Similarly, where automated updating is not available, rectification is available through the controller contacting the processor to perform record amendments on their behalf. All Forensic Information Databases will have a defined data assurance strategy which aims to identify and resolve inaccurate records. Any records that have breached the privacy of one or more individuals will need to be sent through the organisation's Data Protection Officer to consider whether the case needs to be reported to the ICO. An example of this would be an unlawful match or where data from the databases have been used to interview the wrong person (for example where a person has been interviewed resulting from an inaccurate record, such as a sample switch where a sample has been allocated to the wrong PNC result).

The request for creation of a new container within an IDENT1 collection will be through the collection administrator whose role is to ensure presence of a legitimate purpose and authority for creation of the set, that there is an audit trail for the data established, and it will be subject to review to ensure the ongoing relevance of the container. For Ad Hoc containers, the administrator role is NCA where the container is solely for NCA access and use, or otherwise FINDS, on behalf of the Strategy Board. A general consideration for the creation of an Ad Hoc container is that where the function of the records usage is not relevant to the overall purpose of the IDENT1 Unified Collection / Unidentified Marks then an Ad Hoc is to be created; for example, records that are being used for user acceptance testing (UAT) purposes are not permitted to be created directly within the Unidentified Marks/Unified Collection (see Annex V), rather an Ad Hoc container would need to be set up for the specific UAT purpose.

8.5. Control of Access to Forensic Information Databases

No LEA or FSP is authorised to have direct access to the DNA Data held on NDNAD.

For the fingerprint law enforcement collections held on IDENT1, the general principle is that an authoriser of appropriate status within an LEA can grant access to staff; the respective database Security Operating Procedures (SyOps) define requirements and restrictions such that the authoriser is of suitable status as to take responsibility for the Organisation's database user access, and that the staff granted access are deemed competent and have the appropriate access.

- For IDENT1, where a Police Force Information Security Officer is able to assert that their standard policies and procedures covers the requirements stipulated in the SyOps, then there is not a need for their staff to specifically sign off on the SyOps. Where this cannot be asserted, the SyOps are completed and held by the Home Office Product Owner, for audit by the National Policing Information Risk Management Team (NPIRMT).

A small number of staff who are responsible for the day to day management of the Forensic Information Databases and have the relevant access to the system, as appropriate for their role. The designated Information Asset Owners (or responsibility delegated to the controller with respect to fingerprints) ensures that only staff with a legitimate reason for accessing the databases have access and that their access is regularly reviewed.

Members of the public may request access to DNA or Fingerprint Data directly relating to them. All such 'Subject Access Requests' (SAR) must be made to the LEA that originally obtained the DNA sample or fingerprints[20]. The record will only be provided to the individual making the request or an authorised third party representing them. Where third party requests relate to deceased individuals, the definition of personal data only relates to living individuals, and so use of the SAR to obtain information about a deceased individual would not be standard; in these cases the LEA in receipt of the request is to be satisfied that the request is genuine (i.e. the individual is deceased) and that there is either a lawful basis for the release, or the release is specifically for Policing purposes. Relevant information for requesting information is available on the website for the Information Commissioner's Office (ICO).

In respect of automated processing which takes place for Forensic Information Databases, measures must be in place to:

a. deny unauthorised persons access to processing equipment used for processing ('equipment access control');
b. prevent the unauthorised reading, copying, modification or removal of data media ('data media control');
c. prevent the unauthorised input of personal data and the unauthorised inspection, modification, or deletion of stored personal data ('storage control');
d. prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control');
e. ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control');
f. ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control');
g. ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control');
h. prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control');
i. ensure that installed systems may, in the case of interruption, be restored ('recovery'); and

[20] Such information provided by FINDS relates solely to the presence for records on FIND databases and so doesn't include provenance of the sampling and continuity to the point of retention (or subsequently following release of match or other information from FIND databases).

j. ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').

Personal data breach

In the case of a personal data breach, the controller must notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the supervisory authority (in this case, the ICO) and the Strategy Board, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. The specifics for an event should be fully detailed and allow the logical decision taken for where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller (processor) can communicate the personal data breach to the data subject without undue delay.

8.6. Provision of Management Information Derived from the Forensic Information Databases

No Forensic Information Database data, or direct personal identifiable information may be shared through the provision of Management Information.

Management Information data is based on a snapshot of the respective databases at a given time. To ensure the accuracy of the information supplied and to identify any applicable caveats, all management information is subject to quality assurance procedures prior to release. The Strategy Board requires that high level trend analysis management information is available as and when requested to do so. Such information is routinely published in the Strategy Board's Annual Report and through the gov.uk website.

The FINDS may routinely access management information to assess the effective performance of the Forensic Information Databases.

The production and use of management information for Parliamentary Questions (PQs) and Freedom of Information Act (FOIA) responses complies with the Home Office guidance on answering PQs, FOIA, and Data Protection Act requirements.

Members of the public may access further management information via a freedom of information request in line with the Freedom of Information Act 2000 or through the website: https://www.gov.uk/make-a-freedom-of-information-request

8.7. Use of FIND Data for Research

The Strategy Board supports, in principle, the use of data for enhancing the criminal justice, academic and public understanding of the use and impact of the Forensic Information Databases. All requests for accessing data for such purposes must be specifically authorised by the Strategy Board. Decisions will be made on a case by case basis based on the proportionality, necessity, impact on privacy and perceived value of the proposed research. Early consideration of the ethical impact of this research is encouraged. It is of note that the Data Protection Act 2018 (Part 3) does not permit access to personal data if it relates to decisions or measures made in relation to a specific data subject or would cause damage or substantial distress.

In order to apply for the use of data to support this principle, research requests should be submitted using form FINDS-F-067 'Proposal to Conduct Research and Development using Fingerprint and Footwear Images, DNA Samples, Profiles and or NDNAD, IDENT1 or NFD Data' with the accompanying Process for Release from the Forensic Information Databases and the National Footwear Database for Research purposes.

The FINDS Unit shall maintain a register of all research applications and the corresponding Strategy Board decisions.

8.8. Records and Audits of Access and Use of FIND Data

FINDS, Forensic Units (including FSPs), and LEAs are required to maintain records/logs and audit their access and uses of data that is sampled for storage or searching against the Forensic Information Databases.

Such records are to be kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination, and erasure. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data. The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings. The controller and the processor must keep the logs and make them available to the ICO on request.

Forensic Units, including FSPs, are required to demonstrate their compliance to this policy. Although this is primarily achieved through third party auditing by the United Kingdom Accreditation Service (UKAS) against the international standard for testing laboratories, ISO 17025 and the NDNAD specific standard LAB32[21], FSPs must provide such records to the Strategy Board, FINDS, and/or the Forensic Science Regulator on request.

Forensic Units failing to comply with this policy will have their authorisation to load records to, and receive data from, the respective Forensic Information Database(s) reviewed.

8.9. Data Protection Impact Assessments for Forensic Information Databases

With the operation of Forensic Information Databases being in concordance to the type of processing likely to result in a high risk to the rights and freedoms of individuals, there is a requirement under the Data Protection Act 2018 (Part 3) for a data protection impact assessment (DPIA) to be undertaken by the controller. This is an assessment of the impact of the envisaged processing operations on the protection of personal data for each type of processing carried out by a controller; in practice, this would be carried out for each database, and the DPIA may be compiled by the processor on behalf of the controller. The DPIA must consider the nature, scope, context, and purposes of the processing and must include the following:

- a general description of the envisaged processing operations;
- an assessment of the risks to the rights and freedoms of data subjects;

[21] LAB32 is the requirements for accreditation of suppliers to the NDNAD

- the measures envisaged to address those risks; and
- safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

Where the DPIA concludes that the processing would (in the absence of any mitigation) be likely to incur a high risk to the rights and freedoms of data subjects, there would be a need to provide a copy of the DPIA, and any other relevant information, to the Information Commissioner's Office.

A scheduled review of the data protection impact assessment should also be undertaken to ensure that there is continued adherence.

8.10.International Agreements

Where international agreements are in place which relate to the Forensic Information Databases access and usage principles of this document, there should be transparency of this information through ensuring that the Strategy Board (through communication to FINDS) are sighted. FINDS-P-040 'International DNA and Fingerprint Exchange Policy for the United Kingdom' provides the full detail for international aspects.

Annex I - Law Enforcement Agencies (LEAs) Permitted Access and Use of DNA Samples, DNA Profiles, Fingerprint Images, and Associated Data

General definitions - LEAs

Territorial Police Forces - England & Wales	
Avon and Somerset Constabulary	Lincolnshire Police
Bedfordshire Police	Merseyside Police
Cambridgeshire Constabulary	Metropolitan Police
Cheshire Constabulary	Norfolk Constabulary
City of London Police	North Wales Police
Cleveland Police	North Yorkshire Police
Cumbria Constabulary	Northamptonshire Police
Derbyshire Constabulary	Northumbria Police
Devon and Cornwall Constabulary	Nottinghamshire Police
Dorset Police	South Wales Police
Durham Constabulary	South Yorkshire Police
Dyfed-Powys Police	Staffordshire Police
Essex Police	Suffolk Constabulary
Gloucestershire Constabulary	Surrey Police
Greater Manchester Police	Sussex Police
Gwent Police	Thames Valley Police
Hampshire Constabulary	Warwickshire Police
Hertfordshire Constabulary	West Mercia Police
Humberside Police	West Midlands Police
Kent Police	West Yorkshire Police
Lancashire Constabulary	Wiltshire Constabulary
Leicestershire Constabulary	

Territorial Police Forces – non- England & Wales
Police Scotland
Police Service of Northern Ireland
Guernsey Police
States of Jersey Police
Isle of Man Constabulary

Special Police Forces and Other Organisations
British Transport Police
Service Police Crime Bureau/Royal Military Police
Scottish Crime & Drug Enforcement Agency
Ministry of Defence Police
National Crime Agency
HM Revenue and Customs
ACRO Criminal Records Office[22]
(NCA) UK Protected Persons Service
Scottish Police Authority

[22] ACRO provide PNC services for Non-Police Prosecuting Agencies

Annex II - General Access and Use by specific Forensic information database

	Forensic information database	
Category	**DNA NDNAD**	**Fingerprints IDENT1[23]**
Territorial Police Forces - England & Wales	✓	✓
Territorial Police Forces – non-England & Wales	✓	✓
Special Police Forces and Other Organisations	✓	✓
Organisations authorised to process data to support the operation of the Forensic information database	FINDS[24]	• FINDS • UK Visas & Immigration (IABS/ICFN) • ACRO Criminal Records Office • Scottish Police Authority[25]
Organisations authorised to receive data, and request specific searches to be performed, from the Forensic information database	• Criminal Cases Review Commission • Immigration Enforcement, Criminal and Financial Investigation unit • Royal Mail[26] • Department of Work and Pensions[25]	ACRO provide PNC services for Non-Police Prosecuting Agencies
International Law Enforcement Agencies	✓ Requirements defined in FINDS-P-040 'International DNA and Fingerprint Exchange Policy for the United Kingdom'	✓ Requirements defined in FINDS-P-040 'International DNA and Fingerprint Exchange Policy for the United Kingdom'

[23] Specifically, the fingerprint collections in IDENT1 used for law enforcement purposes

[24] 'FINDS' is the Forensic Information Databases Service - the Home Office unit authorised to process data to support the operation of Forensic information databases.

[25] Specifically, for deletion of Scottish records

[26] Royal Mail and Department of Work and Pensions will submit DNA samples for profiling through a Law Enforcement Agency.

Annex III - Expanded process, defining stakeholders, data ownership, authority, and lawful purpose

DNA	Overall process, defining stakeholders, data ownership, authority and lawful purpose			
	Collection	Analysis	Database interactions	Investigation
Sample source	• Arrestees/detainees • Missing Persons • Vulnerable Persons • Voluntary Attendees • Volunteers –Elimination • Volunteers – Kinship • Crime Scenes/Unidentified bodies • For contamination elimination purposes • International LEAs (through NCA)	Not Applicable	• Crime stain records • Arrestees/detainees • Counter Terrorism • Vulnerable Persons • Contamination/Elimination (CED & PED) • Missing Persons Outputs to LEA/FSP Forensic Units, DWP/ Immigration Unit, or international partners through NCA	Not Applicable
Stakeholder/ actor	• LEA • Border Force & National Ports Police (detainees only)	Forensic Service Provider (by approval through Strategy Board, ISO17025 and FSR Codes of Practice)	• Home Office • Metropolitan Police Service	LEA
Data ownership	Controller	Processor	Processor	Controller
Lawful Purpose	PACE/TACT (TACT Section 7 – detainees) For elimination collections - Police Regulations for Officers, T&Cs for Police staff	PACE/TACT (through contractual arrangements)	Statement of Requirements	PACE/TACT
Jurisdictions	• England and Wales • Scotland • Northern Ireland	• England and Wales • Scotland • Northern Ireland	National	• England and Wales • Scotland • Northern Ireland

Fingerprints	Overall process, defining stakeholders, data ownership, authority and lawful purpose			
	Collection	**Analysis**	**Database interactions**	**Investigation**
Sample source	• Arrestees/detainees (Unified Collection) • Immigration (IABS) • MOD (BLADE) • SCORD (CT) • Missing Persons • Vulnerable Persons • Voluntary Attendees • Volunteers – Elimination • Crime Scenes/Unidentified bodies • For contamination elimination purposes • International LEAs (through NCA) • Ad Hoc and ORD	Not Applicable	• Crime stain records • Arrestees/detainees • Counter Terrorism • Vulnerable Persons • Contamination/Elimination • Missing Persons • BLADE • Specialist Collections Outputs to LEA Forensic Units, LEA CT Units (for BLADE Interactions with Policing collections), ACRO, MOD/DSTL, or international partners through NCA.	Not Applicable
Stakeholder/ actor	• LEA • Border Force (detainees only) • UKVI for Immigration	LEA Bureau (by approval through Strategy Board, currently working to gain accreditation to ISO17025 and FSR Codes of Practice)	• Home Office • Metropolitan Police Service • Ministry of Defence	LEA
Data ownership	Controller	Processor	Processor	Controller
Lawful Purpose	• PACE/TACT (TACT Section 7 – detainees) • Immigration Act for Immigration purposes • MOD legislative frameworks (for BLADE) • For elimination collections - Police Regulations for Officers, T&Cs for Police staff	PACE/TACT (through contractual arrangements) MOD legislative frameworks (for BLADE)	• PACE • Statement of Requirements	PACE/TACT
Jurisdictions	• England and Wales • Scotland • Northern Ireland	• England and Wales • Scotland • Northern Ireland	National	• England and Wales • Scotland • Northern Ireland

Annex IV - FIND Strategy Board Regulation/Oversight model

DNA					
Activity	**Database processor/ Authority**	**Strategy Board**	**Biometrics Commissioner**	**Information Commissioner**	**Forensic Science Regulator**
PACE Arrestees/ Crime stain records	Home Office/LEA	✓	✓	✓	✓ Analysis – ISO 17025 & FSR Codes Databasing - ISO9001, ISO/IEC 20000, ISO/IEC 27000 series (as provided through the TickIT*plus* scheme)
TACT subjects and crime stain records	MPS/ LEA where sample taken	✓	✓	✓	✓ Analysis – ISO 17025
Detainees – TACT Schedule 7	MPS/LEA where sample taken	✓	✓	✓	✓ Analysis – ISO 17025
Missing Persons	Home Office/Missing Persons Unit	✓	✓	✓	✓ Analysis – ISO 17025 & FSR Codes Databasing - ISO9001, ISO/IEC 20000, ISO/IEC 27000 series (as provided through the TickIT*plus* scheme)
Vulnerable Persons	Home Office/LEA	✓	✓	✓	✓ Analysis – ISO 17025 & FSR Codes Databasing - ISO9001, ISO/IEC 20000, ISO/IEC 27000 series (as provided through the TickIT*plus* scheme)
Volunteers	Home Office/LEA	✓	✓	✓	✓ Analysis – ISO 17025 & FSR Codes Should not be loaded, unless due to kinship comparison for MPDD
Contamination Elimination Databases	Home Office/LEA	✓	✓	✓	✓ Analysis – ISO 17025 & FSR Codes Databasing - ISO9001, ISO/IEC 20000, ISO/IEC 27000 series (as provided through the TickIT*plus* scheme)

Fingerprints					
Activity	**Database processor/ Authority**	**Strategy Board**	**Biometrics Commissioner**	**Information Commissioner**	**Forensic Science Regulator**
PACE Arrestees/Crime stain records	Home Office/LEA	✓	✓	✓	✓ Analysis – ISO 17025 by 2018 Databasing - ISO9001, ISO/IEC 20000, ISO/IEC 27000 series (as provided through the TickIT*plus* scheme)
TACT subjects and crime stain records	MPS/ LEA where sample taken	✓	✓	✓	✓ Analysis – ISO 17025 by 2018
Detainees – TACT Schedule 7	MPS/LEA where sample taken	✓	✓	✓	✓ Analysis – ISO 17025 by 2018
Missing Persons	Home Office/Missing Persons Unit	✓	✓	✓	✓ Analysis – ISO 17025 by 2018 Databasing - ISO9001, ISO/IEC 20000, ISO/IEC 27000 series (as provided through the TickIT*plus* scheme)
Vulnerable Persons	Home Office/LEA	✓	✓	✓	✓ Analysis – ISO 17025 by 2018 Databasing - ISO9001, ISO/IEC 20000, ISO/IEC 27000 series (as provided through the TickIT*plus* scheme)
Volunteers	Home Office/LEA	✓	✓	✓	✓ Analysis – ISO 17025 by 2018
Contamination Elimination Databases	Home Office/LEA	✓	✓	✓	✓ Analysis – ISO 17025 & FSR Codes Databasing - ISO9001, ISO/IEC 20000, ISO/IEC 27000 series (as provided through the TickIT*plus* scheme)
BLADE/MOD	DSTL/MOD	X	X	✓[27]	X
IABS	Home Office	X	X	✓[27]	X

[27] Under the supervisory authority conferred with the implementation of the Data Protection Act 2018 (Part 3)

Annex V IDENT1 Operational and Governance model