

# LEDS/HOB OPEN SPACE CIVIL SOCIETY ANNUAL REPORT – JULY 2018 – MAY 2020

*Final Version*

## CONTENTS

1. Executive Summary .....	2
2. Introduction .....	3
3. Open Space Participants.....	5
4. Activities July 2018 – May 2020 .....	6
5. Impact of process .....	9
• Data Protection Impact Assessments (DPIA) .....	9
• Custody Image Policy.....	10
• Data Sharing .....	10
• Data Quality .....	11
• Data Retention .....	11
• Individual Rights.....	12
• Access Levels & Controls.....	12
• National Register of Missing Persons (NRMP) .....	12
• Additional discussion areas .....	13
6. Looking forward.....	14
7. Appendix .....	15
• Appendix A - NLEDP & HOB Programme Structures .....	15

## 1. EXECUTIVE SUMMARY

This report outlines an engagement process between civil society organisations and two Home Office teams working on law enforcement data and biometrics. The process is called the LEDS/HOB Open Space.

The Open Space was initiated by the Home Office, working with a small number of civil society organisations (CSOs), in 2018 to establish a productive space where the Home Office and civil society could have safe and productive conversations about the National Law Enforcement Data Programme (NLEDP) and more recently, the Home Office Biometrics Programme (HOB) too.

This report is predominantly drafted by the CSO participants of this Open Space and reviewed for any factual inaccuracies by the Home Office. It outlines who is involved in the Open Space; the areas of discussion; where the CSOs feel they have had impact and areas CSOs recommend the Home Office should focus on further.

The issue areas that the Open Space has discussed and that are outlined in this report are:

- Data Protection Impact Assessments (DPIA) for LEDS & HOB
- Custody Image Policy
- Data Sharing
- Data Quality
- Data Retention
- Individual Rights
- Access Levels & Controls on LEDS & HOB
- National Register of Missing Persons (NRMP)
- Additional discussion areas: this is a list of other areas covered in discussions where report contributors didn't have specific reflections.

The aim is to produce a report like this for the Open Space process on an annual basis.

### **Possible audiences we imagine will be interested in the report include:**

- Civil Society Organisations with a general interest in law enforcement data, but not taking part;
- Internal stakeholders within the Home Office, particularly those not directly taking part in the process; and
- Interested members of the public
- Academics interested in this area

## 2. INTRODUCTION

### Background & Purpose of the Open Space

The Open Space was established by the Home Office, working with a small number of civil society organisations (CSOs), at a workshop on 3rd July 2018 to establish a productive space where the Home Office and civil society could have safe and productive conversations about the National Law Enforcement Data Programme (NLEDP). The purpose of the Open Space is not to make policy, but to be part of a wider, more open consultation that the Home Office is doing on NLEDP. Formal consultation and usual approval processes still apply.

At this workshop, participants agreed on the scope of the process and the principles of working together, which are outlined below. The Home Office Biometrics Programme (HOB) was brought into the scope of the process on agreement from all participants in October 2018.

Participants agreed that the Open Space would focus on the following areas of the programmes:

- Governance, inspection and oversight;
- Code of Practice;
- Staff capacity, capability and training;
- Data retention
- Custody image policy;
- Data sharing;
- Data quality; and
- The Data Protection Impact Assessments.

The Open Space has the power to bring in new areas of both programmes as agreed by participants in the space. Should participants agree, the scope of the programme beyond LEDS and HOB can be expanded. This is demonstrated in Section 4 of this report which lists the areas now in scope of the Open Space process. The Open Space is facilitated by [Involve](#), an independent public participation charity.

If successful, the proposed process will contribute to the development of an ongoing process of collaboration between the Home Office, CSOs and organisations from other sectors.

### *Agreed Principles of Working Together*

All participants agree to:

- **Open collaboration:** engaging constructively in the process within the shared purpose of the process. In cases of significant disagreement, Involve will play a mediation role;
- **Engage early:** providing information, data and papers in good time, and identifying significant challenges and blocks as early as possible;
- **Agree to disagree:** not expect consensus on every issue, but to seek to identify, reach agreement on and seek solution to areas of disagreement;
- **Maintain confidentiality:** talking about the process and broad issues discussed as required without identifying individual positions or publishing confidential or embargoed material. In addition, participants agree to not identify the involvement of CSOs to others outside the process without the express permission of the organisation/s concerned;
- **Focus on the process:** engaging on issues of relevance to the scope of the process. This will not prevent organisations from engaging on wider issues and policies outside the space; and
- **Promote accessibility:** identifying and proposing the involvement of participants with a legitimate interest and expertise to engage.

## Background & Purpose of the Annual Report

This is the first LEDS/HOB Open Space Annual Report to be produced and covers the first 2 years of the process. The report will be produced annually from this point forward.

The purpose of the LEDS/HOB Open Space Annual Report is to provide transparency about the discussions within the Open Space; identify progress and sticking points from the point of view of CSOs and to hold the Home Office accountable for its commitments from the process to date.

The report will also ensure that potentially interested stakeholders, both inside and outside of the Open Space, find out more about the process. We hope this in turn may help to bring more organisations into the process strengthening it in terms of the knowledge and skills it is able to draw on.

### *Report Contributors*

Sections 1 - 4 of this report have been drafted and reviewed by Involve who facilitate the Open Space (more detail explained below). These are sections covering the practical aspects of the Open Space.

Civil society participants have drafted sections 5 and 6 explaining their perspectives on the impact of the process and areas CSOs feel the space needs to focus on in future. Involve has reviewed these sections to ensure a balance in terms of input from the different CSOs contributing to the report.

The Home Office has reviewed the whole report for any factual errors otherwise they have not been involved in drafting the main content of this report.

### 3. OPEN SPACE PARTICIPANTS

#### Involve

Involve's role is to hold the space open to allow the Home Office and civil society participants to have productive discussions. In order to do this, Involve does not take sides and aims to structure the workshops and discussions in such a way that everyone can participate fully. Involve is there to ensure participants have a chance to agree or disagree with decisions made. Involve's role is also to hold the Home Office accountable for acting on the discussions and decisions. In case of significant conflict or disagreement, Involve will attempt to mediate provided both sides are acting in good faith.

Involve is mindful that civil society capacity to engage in the process is limited. Another part of Involve's role is to attempt to design a flexible process that means that CSOs can engage in those areas of the two programmes where they have most interest and are able to contribute effectively.

Involve reserves the right to withdraw from this role if it judges that either side is not acting in good faith.

#### Home Office Participants

##### *National Law Enforcement Data Programme*

The National Law Enforcement Data Programme was established to protect the public by building a modern and affordable Law Enforcement Data Service to replace the Police National Computer and the Police National Database and to create a National Register of Missing Persons. Further detail is explained in Appendix A.

NLEDP staff involved in the Open Space: Director Data and Identity Directorate; Head of Data Policy Unit; LEDS Policy Lead, Data and Identity Directorate; Public Protection Portfolio Compliance Lead; LEDS Open Space Project Manager; LEDS Open Space Co-ordinator and LEDS Product Owner.

##### *HOB Programme*

The HOB Programme has a responsibility to provide biometrics related services to a wide range of users, across the Home Office and law enforcement agencies in supporting immigration and law enforcement. Further detail is explained in Appendix A.

HOB Programme staff involved in the Open Space: Senior Responsible Owner; HOB Programme Director; HOB Technical Lead; HOB Open Space Co-ordinator.

#### Civil Society Participants

In total, 24 CSOs have taken part in some or all of the Open Space workshops over the past 18 months. These CSOs have been invited to take part on the basis of their expertise in the use and the impact of the use of data held by police for law enforcement purposes. They include CSOs working on: human rights; privacy and civil liberties; victims' rights and safety; groups working with vulnerable people who may be affected by this work; and wider data issues. To support the sharing of confidential and embargoed material and ensure frank and open exchange of views it has been agreed that individual CSOs will not be identified during the process or within this report except with the express permission of the organisation/s concerned.

## Regulatory & Oversight Body Participants

HMICFRS have been invited to attend Open Space sessions. Inspection of law enforcement use of LEDS is expected to be provided by Her Majesty's Inspectorate of Constabulary Fire and Rescue Services (HMICFRS). The inspectorate covers the geographic police forces in England, Wales and Northern Ireland, additionally they also inspect: non-territorial services, such as British Transport Police and Ministry of Defence Police; specialist agencies, such as HM Revenue & Customs and the National Crime Agency; and international police forces, such as the Isle of Man, Guernsey and Jersey Police. HMICFRS had previously audited police forces on their use of the PNC. In 2011, the Government's Independent Advisor on Criminality Information Management recommended that HMICFRS's audit role was extended to cover all PNC users. More information is available [here](#).

The Information Commissioner's Office (ICO) and representatives of the Biometrics Commissioner have both been involved in Open Space discussions as observers. The ICO is the independent regulator for information rights legislation and oversees the implementation of data protection legislation. The Biometrics Commissioner is independent of government and the Commissioner's role is to keep under review the retention and use by the police of DNA samples, DNA profiles and fingerprints. The ICO has also provided input into NLEDP, including providing advice on data protection considerations in its development and latterly, to the Code of Practice, as well as the Data Protection Impact Assessment.

## Policing Personnel Participants

Within the Home Office many Policing programmes have representation from the police community embedded within the delivery teams. The Operational Communications in Policing (OCiP) team is independent of but attached to the Home Office. It comprises a number of serving police officers and staff who work to the National Police Chiefs' Council. Members of the OCiP team have attended all Open Space meetings to provide operational context and advise on why things are needed and to receive feedback from the Open Space.

## College of Policing

The College of Policing was established in 2012 as the professional body for everyone who works for the police service in England and Wales. The purpose of the College is to provide those working in policing with the skills and knowledge necessary to prevent crime, protect the public, and secure public trust. The College has three main functions; developing research and evidence into 'what works' for policing, supporting the professional development of individuals in policing and setting standards of professional practice and development, including codes of practice and Authorised Professional Practice.

The College was commissioned by the Home Office to create a Code of Practice for LEDS, working closely with NLEDP, and the authors have participated in Open Space. The College will also design the training standards for LEDS and develop the supportive learning programme. The College is currently producing a code of practice for the management of policing records, which is also of interest to Open Space.

## 4. ACTIVITIES JULY 2018 – MAY 2020

Over the last 2 years, participants in the Open Space have discussed and fed into the following areas of both LEDS and HOB.

Output	LEDS	HOB
Governance, Inspection & Oversight	Yes	Yes
Code of Practice & Training	Yes	N/A
Data Protection Impact Assessments (DPIA)	Yes	Yes
Custody Image Policy	Yes	N/A
Data Sharing	Yes	Yes
Data Quality	Yes	No
Data Retention	Yes	No
Access Levels & Controls	Yes	Yes
System Demonstrations	Yes - Demonstration of LEDS capabilities	Yes - Strategic Mobile Equipment Demonstration
Audit Process	Yes	Yes
National Register of Missing Persons (NRMP)	Yes	N/A
Overall Open Space Process	Yes	Yes

### *The Process*

The Open Space process has consisted of 9 workshops up until the date of drafting this report in: July, October & December 2018; February, May, July & September 2019 and January & April 2020 (an online workshop due to Coronavirus restrictions).

Workshops have been a mixture of half day and full day workshops covering a range of the Open Space focus areas outlined above. Papers are produced by the Home Office (or by Involve if relating to the Open Space process itself) and circulated to CSOs ideally at least two weeks prior to the workshop. There have been delays to papers in some instances. When this happens, Involve will always try to alter the process to ensure CSOs have time to engage with the material being discussed during the workshop.

Workshops consist of presentations from the Home Office, plenary discussions and detailed table discussions. Table discussions involve Home Office representatives with responsibility in the area under discussion, CSOs and regulatory/oversight bodies present on the day.

Plenary and table discussions are minuted and a write up is produced from each workshop by Involve which is circulated to all organisations that are part of the Open Space.

### *Core Documents for the Process*

Critical to the functioning of the space is that the Home Office is accountable to the civil society participants for acting in good faith on the discussions in the workshops and other elements of the process. Key to this are three documents:

- Action log – this document captures every action agreed to during the process and tracks progress against each action. There are a significant number of actions and it is structured in a way to try to support civil society participants to identify the actions which are critical for them in order to support them to track progress. Involve's responsibility is to ensure that every action is captured at a workshop, and progress updated. CSOs are responsible for identifying those actions they wish to focus on during the workshops; the Home Office is responsible for regularly updating the log to demonstrate progress to date.
- Open Space Outputs and Progress paper – this brief document captures the core outputs from the process. It is through contributing to the structure and content of these outputs that civil society participants will shape both Leds and HOB. This paper identifies the progress made in developing the output; the date for the next discussion; the key outstanding issues; the papers which have fed into its development so far; and the actions from the action log which relate to its development. The outputs in this document are those listed above.
- Terms of Reference - this document outlines the agreed scope and principles of working for the process. This document is then shared with any new participants joining the Open Space.



## 5. IMPACT OF THE PROCESS

This section provides a narrative from CSOs on the impact of the Open Space on output areas from the NLEDP and HOB Programme discussed in the Open Space. This narrative also identifies any key sticking points, concerns about lack of progress or areas of disagreement between Open Space participants.

### Data Protection Impact Assessments (DPIA)

#### *Issues discussed*

Much of the discussion on DPIAs has involved what should be included in a DPIA. For example, these have focused specifically on the requirements that stem from the Data Protection Act 2018 and the General Data Protection Regulation, or taking a more holistic approach such as including public acceptance and public perception. Further discussions included whether to discuss potential future applications, such as facial recognition and predictive policing, or focus on current data processing practices and what those terms meant. The previous publication was in the format of a Privacy Impact Assessment published in 2018.

A draft of the DPIA mitigations section was presented to available Open Space members in March 2020. Within the mitigations presentation, issues around the nature of the data governance of LEDS were of primary concern, in particular:

- Who will have access to LEDS?
- A definitive list of users and what roles they will have in the system and the data sets (controller, joint-controllers, processors).
- Where joint controllership is in place and the ability for one controller to bind another in their processing.

#### *Impact on developing policy*

CSOs advised the Home Office to focus specifically on the legal requirements of a DPIA, rather than including the wider holistic areas of public acceptance. CSOs also advised the Home Office to detail existing processing applications and then provide subsequent updates for consultation on other areas such as facial recognition or predictive policing. For the latter two areas it was emphasised that these two processing practices would need particularly focused and clear DPIAs as they engage sensitive and contentious processing practices that would need to be considered very carefully rather than bundled in with the general LEDS processing that is currently undertaken. The Home Office clarified on this point that LEDS will not undertake predictive policing or facial recognition. It will undertake facial matching which is comparing two images to determine if they are likely to be the same person.

The Home Office has shown a willingness to listen to and respond actively to the issues raised in mitigation. For example, in previous Open Space workshops where some had raised concerns about law enforcement access to personal data held by the DVLA, the Home Office responded by establishing that personal data will not be transferred from the DVLA. Instead an API that allows LEDS to query DVLA rather than providing multiple copies of the database in various places will be used. Discussions have started but more work is required with vulnerable groups such as children and or child migrants. The Home Office is looking to develop this area in future as a result of having more focused discussions with relevant civil society organisations.

#### *Sticking points and outstanding issues*

Determination of the data controller and processor relationships and future governance once LEDS is live is still required. Further engagement is also needed on the full Data Protection Impact Assessments following the mitigations section discussion.

Given the last Privacy Impact Assessment has very late comments added to it, early engagement with a draft is of key interest for CSOs.

Further and deeper considerations would also be needed on the National Register of Missing Persons. This would include the purposes and target stakeholders, especially whether those stakeholders need to include more than law enforcement and whether other organisations such as charities should also be involved.

## Custody Image Policy

### *Issues discussed*

Custody image policy has been an area of focus for CSOs, crucially the deletion of custody images of unconvicted individuals as is required from the decision by the High Court in RMC from 2012. CSOs emphasised the need for this to take place before significant development of LEDS.

### *Impact on developing policy*

The Home Office confirmed a change in approach when it comes to custody images, from a policy of retention by default, to deletion by default. This has been a positive change that CSO groups have welcomed.

Throughout 2019, police forces have demonstrated and explained the proposed deletion activities and the progress of these activities. This has allowed clarity on both the technological and institutional changes that need to take place to implement a new custody image policy.

A combination of the discussions in Open Space and work by parliamentary committees has led the Home Office to start the custody images review process in August 2019. Some of the initial scoping took place in 2019, but the work began in earnest in 2020.

The Home Office are actively consulting their teams on how to incorporate the judgement from the [Gaughran](#) case into their work programme.

### *Sticking points and outstanding issues*

The actual deletion process has yet to begin despite it being almost eight years since the High Court of England and Wales had clarified the law. It is important for CSOs to see that process begin as soon as possible.

## Data Sharing

### *Issues discussed*

CSOs raised a number of concerns about how information will pass between different agencies who have access to LEDS. They questioned whether information uploaded onto the system for one purpose (for example safeguarding) could later be used for law enforcement or immigration enforcement purposes.

One CSO suggested it would not be acceptable for information provided by the public or a reporting person to help find a missing person to be used for immigration enforcement. Doing so would erode public trust in the police; prevent some vulnerable people from being reported missing; and risk CSOs being limited in how they work with the police. The CSO requested a public statement on how information will be shared between different elements of the new system, and a commitment from the relevant Minister to guarantee that information provided for safeguarding isn't misused.

### *Impact on developing policy*

The Information Commissioner's Office (ICO) confirmed that purpose limitation is a key principle in data protection legislation and further processing of personal data shouldn't be incompatible with the original purpose(s) data was collected for. It would therefore depend on what the original purpose(s) personal data on LEDS have been collected for to work out whether further processing was compatible/ incompatible. NLEDP representatives confirmed that they would consider this further.

### *Sticking points and outstanding issues*

There has been no public statement as of yet on how information provided for safeguarding reasons will be used.

## Data Quality

### *Issues discussed*

Data Quality and the importance of it for LEDS has been a key theme of Open Space discussions. The Home Office has demonstrated the work it is doing to support policing in understanding the quality of data currently on both the Police National Database and the Police National Computer. The Home Office states the Information Assets Dashboard is now provided to over 80% of police forces (including non-Home Office forces), with the remaining due to be created by July 2020. The Home Office has discussed some of the key data quality trends both good and bad and were able to show how LEDS does what it can to mitigate any potential risk.

### *Impact on developing policy*

There were no reflections from Report contributors on this point.

### *Sticking points and outstanding issues*

There were no reflections from Report contributors on this point.

## Data Retention

### *Issues discussed*

The issue of Data Retention closely interacts with the Custody Image Policy. Where the Custody Image Policy is a question of how suitable deletion of a category of personal data that is no longer lawful to retain will occur, Data Retention explores the policies going forward.

The European Court of Human Rights judgement in the Gaughran case was an area of discussion in early 2020. The decision confirmed that a policy of indefinite retention of personal data for individuals convicted of recordable offences is a breach of the Article 8 of the right to privacy. This leaves questions about systems design going forward, and the Management of Police Information (MOPI). A further case, [QSA, BROADFOOT and ARB](#) (known as Broadfoot, a Court of Appeal case), raises questions regarding the right to hold data on the Police National Computer, and the current retention periods.

Retention of convictions/cautions hasn't been discussed despite an Open Space participant pressing for this.

### *Impact on developing policy*

### **High level summary of the impact of the discussion on developing policy**

The Home Office is working to ensure LEDS is being built flexibly to adopt any future decisions on retention.

The Home Office are openly approaching the MOPI review as a root and branch review of all information assets that the Police retain. This is a significant commitment from the Home Office that has been welcomed by Open Space attendees.

### *Sticking points and outstanding issues*

The Home Office are due to meet their legal representatives to incorporate the judgement of Gaughran and Broadfoot, so the actual terms of any changes and how that is to be managed still need to be presented to Open Space participants.

The Home Office has recently brought an Open Space participant (who was pressing for engagement around this area in particular) into further discussions with the PNC retention group. More of these discussions need to be brought to the Open Space workshops as a whole in future.

## Individual Rights

### *Issues discussed*

The decision in the Gaughran case has also raised questions, specifically with regard to individual's rights to request deletion of custody images. In the Court's judgement, the level of safeguards, and access to individual rights (requesting deletion) was considered so narrow as to be hypothetical.

### *Impact on developing policy*

The Home Office accepts the need to improve the individual rights regimes and are working with ACRO to understand what they can do better with regard to contact with the public and their rights.

### *Sticking points and outstanding issues*

The Home Office will send documents for future workshops sharing information on an individual's rights and are encouraging Open Space contributions on how to improve that document.

## Access Levels & Controls

### *Issues discussed*

In previous Open Space meetings there were concerns raised about the level of access to personal data, and the scale of access for 3rd party, non-policing organisations. Discussions have also included why a person's data might appear on LEDS.

### *Impact on developing policy*

Specifically, where some had raised concerns about the level of access to personal data from the DVLA, the Home Office responded by establishing that driver licence data will not be transferred from the DVLA, instead an API that allows LEDS to query DVLA data rather than providing multiple copies of the database in various places, as mentioned in the DPIA section above. The Home Office explained this was directly because of those discussions in Open Space.

### *Sticking points and outstanding issues*

There were no reflections from Report contributors on this point.

## National Register of Missing Persons (NRMP)

### *Issues discussed*

CSOs flagged potential issues with the quality of data if inputting into the new system reflects current practice with other policing systems. This would be concerning if practice was inconsistent across different forces as the presence or lack of information might inform safeguarding. For example, if one force does not consistently upload information about vulnerability and another does, the second may assume there is no vulnerability and act inappropriately if someone from the first force is found in their area and a check of the NRMP is carried out. Poor data quality could have other adverse effects and would certainly decrease the system's value as a tool for understanding the national picture of missing.

### *Impact on developing policy*

NLEDP representatives informed the CSOs of the plans for oversight of data quality which has been thought through at length. However, there are still some questions to be answered about how police forces will be held to account on their use of the system.

### *Sticking points and outstanding issues*

There were no reflections from Report contributors on this point.

### *Additional discussion areas*

We discussed a number of other areas in the Open Space that have not received any comment from the CSOs contributing to this Report. Those areas are:

- Governance, oversight & inspection
- LEDES Code of Practice & training
- Systems demonstrations
- Audit process
- The overall Open Space process

## 6. LOOKING FORWARD

These are the areas CSOs identified as outstanding issues that the Home Office must focus on in future and continue to update the Open Space on:

- Data Protection Impact Assessment has been presented with CSOs able to make comments.
- Custody images review must be completed and deletions begin.
- Code of Practice and public awareness documents are made available providing clarity to members of the public and civil society representatives regarding:
  - The processing undertaken in LEDS.
  - Who has access to data held on LEDS.
  - The rights of an individual whose data has been added to LEDS
- Data retention and internal policies - related to Management of Police Information - are reviewed and proposals discussed with Open Space members.

## 7. APPENDIX

### Appendix A - NLEDP & HOB Programme Structures

#### *National Law Enforcement Data Programme - description provided by the Home Office*

The enhanced services in scope for LEDS feed into one of these six Business Services:

- CHECKING – check background information, check custody status, verify identify, check historic threats and warnings.
- ALERTING – alert management, alert presentation. Ability to set up alerts to be told automatically when a record has been changed; scaling up existing PND functionality and making it available across both data sets. A pilot is currently underway with Offender Managers to understand requirements and inform the design of the alerting capability.
- INSIGHTS – Interrogate (search/explore), Analytics (Pattern, Predictive, Risk), Enrichment (associations) potential for predictive analytics, links with Management of Risk in Law Enforcement (MoRiLE).
- REPORTING – standard Management Information, statistical reporting, user reporting.
- DATA – matching, ingest (updates from forces “Updategrams”, direct data entry) and data management & compliance.
- INFORMATION ASSURANCE – Audit, Authentication, Authorisation (Roles and Attribute Based Access Controls).

Since 1974 PNC has grown to be the backbone of UK policing in respect to everyday checks on identity, threat, status and background. PND has in a much shorter time become a critically important repository of information through which policing and other agencies can share vital intelligence and reports across force and agency boundaries.

There is now a clear need to update how these data services are delivered to law enforcement. PNC is 45 years old and needs urgent modernisation. Furthermore, dividing national data between two separate systems makes management of and access to information inherently inefficient and restricts the information that can be provided to police officers in operational situations. It is also costly to maintain two different systems. Some of the key issues that need addressing are:

- Getting a single view of all the pertinent information relating to a person (and objects) across the two systems is a time-consuming manual process that isn't suitable for immediate front-line checks for emergency responses.
- The systems (PNC in particular) are not easily or affordably adaptable to meet the changing demands or priorities of law enforcement or new legislation. For instance, constraints have made it difficult to evolve PNC to support the safeguarding of vulnerable individuals (an example of this is that it does not retain data about historic missing person events).
- PNC is at the end of its life and the skills and knowledge required to manage it are becoming increasingly limited with security vulnerability growing because of the age of the technology it is delivered through.
- While some PNC and PND data can be accessed on mobile devices, current connectivity limits the extent to which the data can be utilised at the point of need.
- Current user interfaces are not intuitive, meaning lengthy training sessions are required to get the most out of the PNC and PND. This training commitment is difficult and expensive to maintain. Intuitive and efficient data services, such as those commonly deployed on smart phones or through modern web applications, are required employing up to date design approaches that optimise the user experience. By contrast PNC requires users to look through many different screens to view information that could easily be consumed on a single concise page.
- PND has made steps to support automated alerting to users about new events relating to people of interest, such as offenders being managed back into the community. There is

great scope to develop this further across all the national data, which will support early proactive intervention as and when the information that might trigger intervention becomes 'known' and uploaded onto the systems.

Additionally, at present, there is no single system to record and share information about people who go missing. The National Law Enforcement Data Programme (NLEDP) will be working to deliver a National Register of Missing Persons (NRMP). This will provide a snapshot of live missing persons enquiries across police forces in England and Wales. It will help officers when they encounter a missing person particularly if that missing person is outside their home force area.

Placing all of this information into one system will not mean data is available for all users to search. While all the collections of data will be physically in one system, they will be logically separated with role-based access controls (RBAC) allowing user access only to the data and activities they are permitted to access.

### Programme Organisation Structure

The NLEDP Senior Leadership Team (SLT) makes decisions on the day to day running of the programme; non-operational decisions, approval of training and staff events – this is chaired by the Programme Director.

It provides the governance, authority and direction required to ensure alignment of NLEDP resources with the programme strategy, objectives and priorities and to optimise NLEDP investments. The Programme Director is the final decision authority and issues are escalated to the NLED Programme Board and/or the Senior Responsible Owner (SRO).

The NLEDP SLT accountable to the SRO, acts as the key escalation point for any programme risks and issues and has signing authority for spend and reports to the NLED Programme Board.

The SRO (Senior Responsible Owner) is directly accountable to the Chief Operating Officer and Parliament and has personal responsibility for delivery of the NLED Programme. The SRO is authorised to approve expenditure within the programme budget and to agree rescheduling. The SRO chairs and is supported by the NLED Programme Board.

The NLED Programme Board approves changes to scope and scheduling and provides feedback and guidance to the programme. The NLED Programme Board is chaired by the SRO and reports to the Law Enforcement Portfolio Board.

The NLEDP Business Design Authority (BDA) identifies, captures, develops and assures the business requirements; identifies, captures and tracks benefits; resolves business design and business architecture conflicts; and designs and maintains the target operating model. It reports to the NLED Programme Board and informs other wider Home Office BDA's where appropriate.

OCiP (Operational Communication in Policing) operates as a business design authority to ensure there is a 'voice of the Police Service' within NLEDP. OCiP feeds into the NLEDP BDA with a clear police view on issues requiring deliberation. The Head of OCiP sits on the NLED Programme Board.

### *HOB Programme - description provided by the Home Office*

The systems in scope in the HOB Programme that provide such biometric services are:

- IDENT1 (Law Enforcement and Security Biometrics System) – provides biometric enrolment, identification and identity management services within the law enforcement domain, principally for arrestees in the UK, but also covering other specialist data sets.
- Immigration and Asylum Biometrics System (IABS) – provides biometric enrolment, identification, identity management and verification services within the immigration and citizenship domains. E.g. for visa applicants to the UK, biometric residency permit applicants, asylum applicants and passport applicants.
- National DNA Database (NDNAD) – the NDNAD holds DNA profiles of subjects in criminal cases, some of whom have not been convicted of a crime and profiles of victims, as well



as marks from crime scenes. The database also holds DNA profiles of vulnerable persons who fear they may be victims of a crime; volunteers who may be vulnerable to attack themselves if their details become known to the wider public; and police officers for elimination purposes. The missing persons and the contamination elimination databases are currently held on a different infrastructure. However, it is planned that the strategic DNA Service will store all data in a single database made up of multiple, logically separated collections.

- Biometric Accuracy Test (BAT) environment – through the Biometric Accuracy Testing (BAT) environment, HOB has undertaken a full and comprehensive approach to testing to select the most advantageous matcher software, and to provide wider assurances of future biometric capabilities.