NLEDP Open Space Workshop 2 Write Up Thursday 4th October

Actions from the Workshop

This is a record of all actions captured in this write up from the workshop on 4th October.

Actions	*Deadline*
1. Home Office to share high level view of recommendations from the Delivery Review to Open Space participants.	October 2018
2. HO to share list of LEDS users with group.	November 2018
3. HO to clarify if user such as probation services would have access to LEDS.	November 2018
4. HO to bring conversation of Public Consultation on Code back to the group.	December 2018
5. HO to map out different regulatory bodies that will cover LEDS and how this will work with different regulatory processes.	December 2018
6. HO to review if Code will include governance outline e.g. who to go to with whistleblowing concerns.	December 2018
7. Paper on governance to be brought back to a future workshop.	December 2018
8. HO to confirm if there will be access controls for LEDS users in the police for searching family information for example.	November 2018
9. Review missing commitment re. inputting data.	February 2019
10. HO to look at accessibility of the Code and providing hard copy information to users.	February 2019
11. Code of Practice must include a mechanism for how it will be updated, on what basis including responses to inspection regime.	February 2019

12. HO to review all recommendations for Purpose Statement & Commitments and update Code of Practice paper accordingly.	December 2018
13. HO to think about right body to run inspection regime taking into consideration different bodies discussed at the workshop.	February 2019
14. Governance: group want to see which powers have reviewed system.	February 2019
15. HO to use existing Inspection examples to create LEDS Inspection process.	December 2018
16. HO to ask group for recommendations on required record keeping for new data added to system.	May 2019
17. HO to consider and come back to the group on whether there should be an annual report on the stats of use of the system.	May 2019
18. Next stage of inspection regime to be shared with the group.	May 2019
19. Further conversations needed on data sharing and data input to LEDS from external sources.	May 2019
20. Discussion needed in data sharing conversation on how data is shared, if standards for data quality can be enforced on data from external sources & how this data could get on LEDS.	May 2019
21. HO to produce report on what defines an entity on system & session to be held on this at future workshop.	December 2018
22. HO to provide clarity on what from LEDS is/isn't evidence.	December 2018
23. HO to provide explanation of what "intelligence" covers.	December 2018
24. HO to provide explanation of how decision is made as to what data is kept/isn't and what the process is.	February 2019
25. HO to share blank copy of dashboard.	November 2018
26. HO to explain governance around data onboarding.	December 2018
27. Discussion to be had at future workshop on what data should appear on screen for users.	December 2018
28. Discussion to be had at future workshop on HO decision-making for what's included on system.	December 2018
29. HO to share number of records on PNC & PND now.	November 2018
30. HO to share with group when/how person record created.	November 2018
31. HO to bring new system prototypes to future workshops to review again.	February 2019
32. HO come back to how fingerprint match will be highlighted on LEDS.	December 2018
33. Request from group for ongoing process where group knows they can raise and discuss set issues in the longer term.	May 2019

INTRODUCTION

This write-up provides a summary of the discussions and actions from the second workshop in the Home Office's National Law Enforcement Data Programme Open Space process with civil society organisations, facilitated by Involve.

The workshop covered the following areas and this write up outlines the discussions and actions for each area:

- A Programme Update from the Home Office (HO)
- Law Enforcement Data Service (LEDS) Code of Practice
- LEDS Data Inspection
- LEDS Data Quality & Ethics
- LEDS & Evidence
- LEDS System Concept Capabilities Discussion
- Next Steps

Summary of Areas of Focus

The following areas were the overall focus points of discussion either as recurring themes or core requests from participants:

- Accountability: who will be accountable for the system and how will this be enforced?
- Governance: what will the governance structure look like?
- Reporting: what form will the reporting take, how frequent and what will its impact be?
- Balance of risk & benefit throughout whole process: with a greater number of victim support groups in the room, the requirement for balance between risk and benefit was even more evident at this second workshop.
- Regular Programme Updates required: the group requested six weekly updates on programme progress.

Several other issues were discussed during the day. The rest of this paper provides further context to these other issues and the summarised themes above under the following categories:

1. Questions for clarification which were answered
2. Questions/points for consideration that have led to an action captured in this paper
3. Questions/points for the HO to consider as it develops papers/policies

ISSUES DISCUSSED

1. Programme Update from the Home Office

The Home Office provided a short paper updating on the status of the programme and an explanation around future time frames, in part due to a delivery review conducted on the programme.

1.1. Clarifications

There were no questions/points for clarification on this paper.

1.2. Points to be taken into account

The key question raised from this paper asked for the findings from the delivery review to be made available to the group. The Home Office confirmed the high-level view of recommendations from the review could be shared.

1.3. Points for further consideration

There were no further specific points for consideration from this section of the workshop.

Actions	*Deadline*
1. Home Office to share high level view of recommendations from the Delivery Review to Open Space participants.	October 2018

2. LEDS Code of Practice

The Code of Practice paper was discussed in groups and then in plenary form focusing on these two questions:

1. How can the purpose statement be strengthened?
2. Are there ways in which the commitments could be improved?

The below notes were captured from the discussions that followed:

2.1. Clarifications

- Who can access LEDS? A list of users requested by participants so that the group can consider if a further conversation is needed on circumstances of users at a later workshop.
  - HO clarified on this point that LEDS won't affect existing legislation covering users.
- Would a user such as probation services have access to LEDS? HO to clarify this.
- Will there be a period of public consultation on LEDS Code of Practice? HO confirmed there definitely will be within the Open Space and will review and ask for further advice from the group whether there should be a wider public consultation process.
- A suggested missing commitment was regarding training – will there be a national standard for training? Will there be structured training for the system?
  - Manuals, multilayers training: e-learning modules etc which are then linked to access controls.
  - The Home Office has appointed two learning partners one being the College of Policing which should be setting the learning standards for LEDS. The Home Office will explain the links between the Code and the work on training. The Home Office will be able to discuss this at a future workshop.
- Is it feasible to review each year with consultation? What happens if it needs updating outside the annual cycle? Possibly response to an inspectorate report – feeds into J.
  - HO: Yes with current governance plans.
- Will the system be maintained by contractors outside government?
  - Intention for this to be a HO service and contractors to be embedded within HO. Focusing on system building being able to adapt and keep up with changing tech.

2.2. Points to be taken into account

- Will the Code include governance outline e.g. who to go to with whistleblowing concerns? HO will review this along with overlapping remits of different regulatory bodies and how this works in practice. The governance framework for LEDS and what it will look like was a key recurring theme throughout the day which will form a substantive part of a future workshop.
- Is accountability missing? Especially given the focus of it in the second part of the Data Protection Act (DPA)?
  - Agreement in the room this needed to be emphasised. The question was raised whether data governance could be broader to include a human rights perspective too as a separate heading?
- Will there be access controls for LEDS users in the police? Broad statement/policy needed for not searching personal information/information on family members etc.
  - HO to clarify and confirm this.
- Missing a commitment around inputting data e.g. false information, accurate.

- Subject access requests, challenging data held about me, rectifying or deleting data. K & J: how can users/HO communicate to the public they can input when certain users don't have access? HO to clarify.
  - Public need single access point. Needs to be clear what info could get.
  - Access controls could stop users responding to subject access requests.
- Accessibility – information on Code of Practice available on gov.uk etc?
  - What if don't have internet access? HO to look at hard copy info too.
- Can HO commit to public consultation on draft of Code? This was used for draft Code for Investigatory Powers Act and would be recommended by the group.]
- Code of Practice must include a mechanism for how it will be updated, on what basis including responses to Inspection regime.

2.3. Points for further consideration

- Ensure there is an active regime for deletion.
- What safeguards in place to ensure quality and purpose of data? And deletion possibility.
  - HO designing new system to include this functionality and designing governance to reflect this. The continued issue is that individual forces have to delete images (and other data) they no longer need.
- Purpose statement not good for public comms.
- Could there be different Codes for data on victims and perpetrators?
  - HO suggested that this will be covered through strict access controls.
- Could the term "fairness" be expanded? Is it too narrow?
- Improving performance is critical for Code therefore Code should cover inputting data too. Including what data is being inputted = openness = being more explicit about the understanding section.
- Purpose of Code is to make people's jobs easier – making data useful → data minimisation/right data.
- Para. N isn't clear – what is the commitment doing?
- Para G: does this refer to LEDS or its data? Make clearer it's about the system.
- How will the Code hold the HO to account for meeting the commitments?
- How can HO put the Code in the public domain?
  - Gov.uk
  - Through users/stakeholders
- Para 17 death penalty issues need to be considered.
- Para 16 take account of Good Friday Agreement for Northern Ireland.
- Needs to cover professional, legal, journalistic, political & faith.
- How will Code deal with legal changes in jurisdictions?
- Need to talk about data sharing.

Actions	*Deadline*
2. HO to share list of LEDS users with group.	November 2018
3. HO to clarify if user such as probation services would have access to LEDS.	November 2018
4. HO to bring conversation of Public Consultation on Code back to the group.	December 2018
5. HO to map out different regulatory bodies that will cover LEDS and how this will work with different regulatory processes.	December 2018
6. HO to review if Code will include governance outline e.g. who to go to with whistleblowing concerns.	December 2018
7. Paper on governance to be brought back to a future workshop.	December 2018

8. HO to confirm if there will be access controls for LEDS users in the police for searching family information for example.	November 2018
9. Review missing commitment re. inputting data.	February 2019
10. HO to look at accessibility of the Code and providing hard copy information to users.	February 2019
11. Code of Practice must include a mechanism for how it will be updated, on what basis including responses to inspection regime.	February 2019
12. HO to review all recommendations for Purpose Statement & Commitments and update Code of Practice paper accordingly.	December 2018

3. LEDS Data Inspection

In groups again, participants were asked to consider these questions reflecting on the paper:

1. What key issues does the HO need to take into account as it develops the inspection regime?
2. How will civil society judge its success?
3. Specifically, what else might the annual report need to cover?

These are the main points that were highlighted by participants:

3.1. Clarifications

- In response to a question asking about what annual reports are going to be published the HO confirmed that reports will be published for each force inspected and there will be a separate report for LEDS as a whole bringing out the overall themes for the country.
- How is governance structured? Not through parliament?
  - HO owned and will be brought to this group (action detailed above) – HO acknowledged it's a very complex topic and will be an ongoing process. Governance will be linked with Parliament and on Parliamentary record.
  - Could there be a Parliamentary Committee overseeing inspection? Home Affairs Committee where Programme has to go before them annually?

3.2. Points to be taken into account

- HO to think about right body to run inspection regime. Previous e.g. of joint inspections by different regulators shared: HMICFRS (Her Majesty's Inspectorate of Constabulary Fire and Rescue Services and Crown Prosecution Service.
- Need to step back & question what is being reported. Are the right things being reported?
- When looking at governance, group want to see which powers have reviewed system etc.
- What powers do HMICFRS have? Sanction powers?
  - No they don't have these powers: is this a limitation? Can HMICFRS exert public pressure & through National Police Chiefs' Council conventions.
  - Are HMICFRS right place to hold inspection? Too focused on operational output (ignoring human rights/data protection/privacy).
  - How can expectations of inspections be communicated to all organisations?
- Use existing examples to create new Inspection processes.
- Will record keeping show how much new data added etc? Can this be in annual report?
  - HO to bring to group to get recommendations on how/what info to log on this.
  - Need proper tracking & reporting: inspection must be much more than just pulling admin data from back of LEDS.
- Annual report of LEDS: incorporate outcome of inspections throughout the year.
  - Suggesting not a specific report from HMICFRS etc.

- Links clearly with governance piece.
- Should there be an annual report? On the expectations? And/or about LEDS: the stats of use? HO will consider how to respond to this and timing to feed into annual DPIA.

3.3. Points for further consideration

- Would public be happy with system that prevents crime or one that is robust that doesn't work as effectively in crime prevention?
  - HO response: can't be an either/or.
- How will HO ensure what might be issues specific to one organisation don't dictate inspections following year?
- Like idea of thematic inspection.
  - Report coverage – need to be clear what should be in every year & what depends on thematic report.
  - Which organisations been inspected on what?
- What are the public interested in/passionate about?
- Inspections should cover where compliant with law.
- Inspection should look at mission creep in relation to how users are acting.
- ICO provide voluntary inspections etc.
- Biometrics Commissioner – have access to inspections.
- How do regulators become stakeholders of inspection?
- Do we need new Inspectorate or new Terms of Reference?
- What's difference between oversight & inspections?
- How to judge success: metrics around misuse & breaches (acknowledged these will be contextual); does inspection reflect experience?; recommendations implemented?; is work plan being followed?
- Resources available to feed into inspection regime e.g. Women in Prison.
  - If documentation on inspection regime published people can feedback in their own time.
- Need to be clear who the audience is for report & something must be available for the public therefore multiple/suite of reports?
  - Who is publishing & how ensure trust in process i.e. no spin?
  - Need to explore how inspectorate will communicate what it is doing to give confidence to the public.
- Narrative evidence from officers using system & from different agencies will be useful: case studies.
  - Could include recommendations for changes too from users.
- Recommendations necessary in report – these must be SMART.
  - How will they be adopted? Accountability mechanisms? Who will do it & how will they make sure they're adopted?
  - What happens if there isn't funding to deal with recommendations?
- How long should gap be between full inspections for organisations performing well?
- Nothing in paper ensuring inspection system is proportionate.
- Do we judge success on barometer or trajectory?
- Need a clear explanation of: What inspection took place? What powers? What happened?
- Investigatory Powers Inspection piece could be useful resource.
  - Biometrics Annual Report useful too & Surveillance Camera Commissioner.
- If regulatory body doesn't have powers themselves, who can someone contact to raise a concern that isn't HO?
- Academic circles interested in these reports?
- Work plan good idea, but inspection should explore if new analytical tools used, new agencies with access or new datasets included – will we see this in annual report? Explore if it drives improvement.
- Leave potential for unannounced inspections/follow-up.
- Hard to envisage what's being inspected at the moment?
- By agency, how often accessing data? Be useful to see this – breakdown of access members.

Actions	*Deadline*
13. HO to think about right body to run inspection regime taking into consideration different bodies discussed at the workshop.	February 2019
14. Governance: group want to see which powers have reviewed system.	February 2019
15. HO to use existing Inspection examples to create LEDS Inspection process.	December 2018
16. HO to ask group for recommendations on required record keeping for new data added to system.	May 2019
17. HO to consider and come back to the group on whether there should be an annual report on the stats of use of the system.	May 2019
18. Next stage of inspection regime to be shared with the group.	May 2019

4. LEDS Data Quality & Ethics

The discussions were held in plenary format using these questions as prompts for this paper:

1. How can the programme ensure it doesn't increase risks to individual rights?
2. How can ethics be woven into the code of ethics?
3. How manage and monitor technologies using data, and what governance is needed?
4. How do we engage the public so they understand what is happening to the data?

The following questions and conversations were then discussed:

4.1. Clarifications

- What is the purpose of the document?
  - HO want minimum data standard
  - Creating info. Assets dashboard – flags to forces when data below standard: this document will inform this.
  - Provide forces with advice & tools they need for that dashboard to help them identify where data quality is low etc.
  - Inform legislation.
  - Created maturity model with ethics & compliance woven in.
- Who has power to delete that data?
  - Management of Police Information (MOPI) guidance determines retention.
  - Focus is currently on implementing data standards as it stands then looking to use tech. to implement MOPI.
- Will LEDS replace other police systems?
  - 5 core systems now feed into PND – no consistent IT picture. LEDS won't replace these, data will just go to LEDS not PND.
- Record of who inputted data? Yes, fully audited in LEDS. Local force systems are all different though if local systems capture data on user that inputted data, LEDS will, if not LEDS will show the force that uploaded the data. System standards being introduced to improve consistency over time.

4.2. Points to be taken into account

- Foreign user searching – is there any record of this? HO to clarify this.
  - Quality of data coming in from other users is a challenge.
- How is data shared & would we enforce standards for data quality on data from other sources e.g. international sources?
  - National Intelligence Model useful here?
  - Discuss in data sharing conversation.

- In what circumstances does data from external source get on LEDS?
  - How can we challenge data on system held about us?
  - Add to conversation for future workshop.
- HO to produce report on what defines an entity – session needed on this at future workshop. Feeds into data standards work.

4.3. Points for further consideration

- Risk: what is risky behaviour? Will retention functionality change?
  - Ideally yes but still to be reviewed & need to determine how to get consistency across forces.
- Broader ethical conversations/issues not specifically on data feeds into Code of Practice.
- HO emphasised importance of Data Quality area of work.
- Important to look at rights of victims and getting balance in this – need for consistency across forces on this. As Domestic Abuse Bill goes through – need to be aware of the above.
- What value does data present in operational context? Need to focus on this.
- Potential tension: retention vs. collecting sufficient info/data.
- Data Quality linked to retention.
- Need to have systems that comply with DPA & future legislation – needs to be able to adapt with legislation changes.

Actions	*Deadline*
19. Further conversations needed on data sharing and data input to LEDS from external sources.	May 2019
20. Discussion needed in data sharing conversation on how data is shared, if standards for data quality can be enforced on data from external sources & how this data could get on LEDS.	May 2019
21. HO to produce report on what defines an entity on system & session to be held on this at future workshop.	December 2018

5. LEDS & Evidence

In different groups, participants discussed the paper in general and more specifically:

1. What are the key questions this paper raises?

These were then shared in plenary discussions. A summary of this section follows:

5.1. Clarifications

- Deletion: limited access to do this – more access to edit but that's auditable.
- De-commissioning systems requirement for deletion.
- How often is LEDS data used as evidence?
  - PNC data frequently used.
  - Officers asked to explain data at disposal & how that influenced decisions.
- Intelligence can be updated but not changed – logged/audited.
- Victim evidence from Domestic Violence not held on LEDS.
- Global Positioning System (GPS) tracking on LEDS?
  - Yes, but with restriction codes. Specific retention requirements on these.
  - How is data deleted? Depends on risk but flagged to review.
- Content of Comms. Data not on LEDS.
- Focus on not disclosing sources of intelligence.
- Automatic Number Plate Recognition (ANPR) watch list capability in scope for LEDS.
- CCTV kept as evidence but not on LEDS.
- Legacy facial images – new board set up to review this.

  - Focused on governance of holding & deleting images etc.
- Can standards be put in to ensure deletion of images can be done by system?
- Standard requirements for forces commissioning new systems to have this capability.
- Fact vs. opinion – what is the definition of evidence?
  - Paper's definition National Intelligence Model (NIM) – clarifies & assesses quality.
- What is purpose of LEDS? Both fact & intelligence.
- How will LEDS be used in court?
  - LEDS data will be used in prosecutions. This includes records of fact and other information where it meets a threshold of reliability. Processes will be needed to ensure that LEDS users are aware of the source of information and what it represents.
  - LEDS data as evidence of misuse of LEDS.

5.2. Points to be taken into account

- Clarity needed from HO on what from LEDS is/isn't evidence?
- What does "intelligence" cover?
- Building body of evidence: how is decision made as to what data is kept/or not?
  - Danger of just in case scenario.
  - What's the process?
- HO can share blank copy of dashboard with the group.
- What's governance of data onboarding?

5.3. Points for further consideration

- Can soft evidence be challenged in the judicial system?
- Paper based on "instant crime" not longer-term issues e.g. stalking law.
  - To what extent will the information on LEDS support prosecution? E.g. alarm & distress in victim.
- All this will require correct guidance on what needs to be collected, when, why & how to balance against proportionality.
- Patterns not being captured (by officers) therefore crimes not going to court.
- How is LEDS data presented in court tested?
  - & what are implications for new digital platform in criminal justice system & going paperless?
- LEDS must ensure evidence can be challenged.

Actions	*Deadline*
22. HO to provide clarity on what from LEDS is/isn't evidence.	December 2018
23. HO to provide explanation of what "intelligence" covers.	December 2018
24. HO to provide explanation of how decision is made as to what data is kept/isn't and what the process is.	February 2019
25. HO to share blank copy of dashboard.	November 2018
26. HO to explain governance around data onboarding.	December 2018

6. LEDS Concept Capabilities Discussion

The afternoon session for this workshop involved a brief overview of a prototype of the new LEDS. Some of the concept capabilities of the system were demonstrated and then plenary discussions were had discussing the various questions that arose from this demonstration.

These are the key points that were discussed:

6.1. Clarifications

- Safeguarding: can this be used as a warning?
  - Still being discussed when this should be surfaced.
- Restrictions on people searching? And logged?
  - All data behind layer of access controls.
  - Everything that's searched is logged & who searched.
- Search without putting reason in? No.
- Reasons Section are 3 fold: streamlines what data the user gets, helps audit & future investigations.
- Different user will have different reason codes.
- Safeguarding – ailments? Where are these from?
  - Not from medical records of mental health records.
  - Still being discussed & decided.
  - Autism Society suggest markers needed for autism & ethicists argue shouldn't.
- Will this be a generic ID database for almost everyone in UK? E.g. due to driving license field.
  - No. Driving license info. Only searchable as part of a road traffic accident investigation. Held siloed in PNC.
  - Intention for LEDS to talk to DVLA to provide necessary data on a request basis rather than as a daily bulk extract. Will come up in future data sharing conversations.
- Accessible on hand-held/remote devices?
  - Still being decided in what form this will be.
  - This can be done but doesn't mean it should be done.
- Associates – people don't have criminal records?
  - Yes, if those reporting missing people have given details of a contact - consented.
  - Yes, if there's an intelligence report against them.
  - Connection with Associates & how it's surfaced on system is up for discussion.
  - DQ linked to this – could be flagged if doesn't meet DQ standards.
- Retention regimes different for Associates to missing people etc?
  - Yes, but Associates stay as long as person is missing.
    - Removed if missing person removed.
    - Dashboard flags this so forces can remove when needed.
- PNC had Police Constable number on it – linked to officer involved.
  - This still logged but older local systems can't do that now. New systems required to log this.
- Analysts inputting data on PNC in control room not logged at moment – this will be reviewed & logged "on behalf" too.
- Communications: contact details – HO clarified wrong use of word for tab on system, not individual's communications rather their contact details etc. Could be from intelligence report.
- Securely logging off ensured?
  - Single sign-in credentials, time out log off & closing browser logs off.
  - Restricting log-ins to shift times? No: part of strategic audit piece.
- Info from different sources? PND feeds.
  - 120 organisations can have access to LEDS.
  - Where information coming from marked on record so know where uploaded from.
- Could "Wanted" capability be linked with Automatic Facial Recognition (AFR).
  - No. Technologically far from this.
- AFR= computer looks through images to match images (not capability of LEDS).
- Facial matching = probe image in to set of unknown people to identify person.
  - Happens already. Human has to verify identity.
- If intelligence is added to system, marked as intelligence & marked where from – requirement going forward.
- Forces able to edit intelligence? Depends on each force but most have some form of verification before edits confirmed.
  - Have to pass training course & re-take test if don't use system for 6 months in order to do this.
  - Limitations on roles can be implemented too.

- Can you search for addresses? And bring up linked people to that address?
  - Yes.
- Will there be just people's records? Or would there be data on being in a set place at a time? E.g. rally or a march?
  - No.
  - Could be a vehicle at an event – doesn't have to be just person records if person information isn't known.
- Would mobile forensics tools used be on LEDS?
  - No.

6.2. Points to be taken into account

- Conversations needed: what data should appear on screen?
- Discussion needed about HO decision-making for what's included on system etc?
- How many records on PNC & PND now and will it be same on LEDS?
  - Could be less as not all data will be migrated. HO to circulate this info.
- Are there rules as to when person record can be created?
  - Yes, be useful to see how person record created? HO to share with group. Needs to link with governance piece
- Bring new prototypes to next workshops to review again.
- Interface linked with IDENT 1 & Immigration & Asylum Biometrics System (IABS) etc?
  - Yes IDENT 1.
  - Biometrics Service Gateway being built.
  - HO will come back to how fingerprint match will be highlighted on LEDS.
- Request from group for ongoing process where group knows they can raise and discuss set issues longer term.

6.3. Points for further consideration

- Can you search intelligence list? Could be lots of information on there.
  - Considering different tool to do wider search on this e.g. for patterns of behaviour.
- Can you create shadow profiles on people without criminal conviction?
  - How can balance be struck with intelligence to protect victims too?
- Who are contact details available to in searches?
- Addresses – need to consider what needed for/when searchable.
- NFA – No Further Action: could notify people about this using contact details – but do you need that to be searchable?
- Feasible to have contact details on Associates?
  - Person record connected to other person record: needs to be purpose for Association.
- "Local" record? From Local intelligence reports but don't have confirmed national report on this.
  - Links back to what information should be served where?
- If added as Associate as victim of abuse – would record come up 10 years later?
  - Still to be decided = why should this information be shown? Balance of risk & benefit.
- Possible to clarify what info considered intelligence & what is public record? Is it necessary?

Actions	*Deadline*
27. Discussion to be had at future workshop on what data should appear on screen for users.	December 2018
28. Discussion to be had at future workshop on HO decision-making for what's included on system.	December 2018
29. HO to share number of records on PNC & PND now.	November 2018
30. HO to share with group when/how person record created.	November 2018

31. HO to bring new system prototypes to future workshops to review again.	February 2019
32. HO come back to how fingerprint match will be highlighted on LEDS.	December 2018
33. Request from group for ongoing process where group knows they can raise and discuss set issues in the longer term.	May 2019

NEXT STEPS

- Share updated papers with all changes from the discussions at this workshop marked on.
- Home Office to follow up on actions recorded from the workshop and actions to be reviewed at start of December workshop.

Home Office Key Take-Aways

- Accountability: key focus.
  - Data purposes.
- Standards for inputting data.
- Reporting – HO to share proposal on how annual reporting process works.
- Code of Practice: re-write purpose statement and circulate to group.
  - Section needed on human rights
  - Clarity on purpose of Code itself needed.
  - Public consultation? HO to take-away & reflect on this & bring back to the group conversation on how best to do a consultation process.
- Rights of victims must not be lost in efforts to improve deletion regime.
- Inspections – what sanction could/should exist?
  - Need to clarify overlaps between different regulatory bodies.
- Key focus on governance – new data sets brought into LEDS & being able to report back on unlawful access.
  - Governance to be discusses at next workshop.
- Programme Update every 6 weeks. Mid. November for next update.
- Half day workshops confirmed going forward.
- HO invited further feedback from participants as soon as feasible on the papers.
  - Code of Practice HO workshop within a month so useful to have this feedback by then.
- List of organisations to be circulated & why have access & extent of access for context – circulate asap.
- Future iterations of system prototype to be shared at future workshops.
- Greater detail to be shared on set bits of information on system & how will be searchable – to be discussed at future workshops.
- Accountability & governance raised in afternoon session too linking back to morning session focusing on this too.