

## **IMPACT Programme:**

# **Police National Database – Privacy Impact Assessment Report**

*national* **AGENCY** POLICING



© - National Policing Improvement Agency (April 2009)

All rights reserved. No part of this publication may be reproduced, modified, amended, stored in any retrieval system or transmitted, in any form or by any means, without the prior written permission of the National Policing Improvement Agency or its representative.

The above restriction does not apply to police forces or authorities, which are authorised to use this material for official, non-profit-making purposes only.

For additional copies, further information with regard to the Programme, or to enquire about the content of this document, please contact Andrew McConaghy, Policy & Legal Compliance team, IMPACT Programme on 020 7147 8306 or [Andrew.McConaghy@npia.pnn.police.uk](mailto:Andrew.McConaghy@npia.pnn.police.uk).

For copyright specific enquiries, please telephone the NPPIA National Police Library on 01256 602 650.

## Contents

Foreword by the Chief Executive and the IMPACT Programme Director .....	4
Executive Summary .....	5
1.The IMPACT Programme.....	6
2.Privacy Impact Assessments and why the Programme decided to conduct one.....	10
3.Methodology .....	11
4.Privacy features of the PND and associated processes .....	14
5.Findings and recommendations.....	21
6.Review and audit .....	22
Annex A: The Bichard recommendations that the IMPACT Programme is addressing.	23
Annex B: PIA screening questions and answers.....	24
Annex C: List of organisations approached during public consultation.....	39
Annex D: Key principles for ensuring the PND is privacy friendly .....	42
Annex E: PND processes.....	40
Annex F: List of Groups Engaged in Consultation.....	45

**A National Policing Improvement Agency paper  
on behalf of the  
IMPACT Programme**

**Police National Database - Privacy Impact Assessment Report**

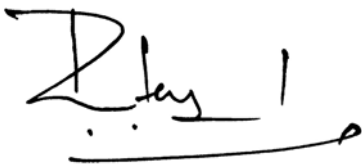
**April 2009**

**Foreword by the Chief Executive and the IMPACT Programme Director**

*The work of the IMPACT Programme is crucial to improving the way that the Police Service manages and shares information, which in turn is crucial to improving the Service's ability to prevent and detect crime, and to make communities safer. These are important goals that will deliver significant benefits not only to the Police Service but also to the public and we are committed to delivering them. However, we are conscious that the management and sharing of information could raise privacy concerns and we are keen to ensure that these are addressed as fully as possible.*

*This report summarises the outcomes of a Privacy Impact Assessment that the Programme has undertaken, the actions that are being taken forward and the stakeholders with which we have consulted. This is only the first, formal, full assessment. It is the intention of the Programme to formally review this report at key milestones during the design and implementation of the Police National Database. However, privacy has been considered throughout the work on the Police National Database and will continue to be as the work progresses.*

*The NPIA is committed to ensuring that privacy is continuously considered across the organisation, and in all aspects of the IMPACT Programme. It is hoped that this report and our continued work successfully demonstrates this commitment to you.*



Peter Neyroud  
Chief Executive



John Crosse  
IMPACT Programme Director

## **Executive Summary**

1. This document sets out the results of a Privacy Impact Assessment focused on the Police National Database aspect of the IMPACT Programme.
2. Section 1 introduces the key work areas of the IMPACT Programme, explains how the Programme sits within the National Policing Improvement Agency (NPIA), and outlines the commitment to the Programme by key stakeholders. It summarises how the Programme was established following the murders of Jessica Chapman and Holly Wells in August 2002, the conviction of Ian Huntley in 2003 and Sir Michael Bichard's subsequent Independent Inquiry.
3. Section 2 outlines why the Programme believes it is important that a Privacy Impact Assessment was undertaken, and how the Programme has conducted this assessment.
4. Section 3 details the methodology employed in consulting and engaging with users, stakeholders and the wider community.
5. Section 4 takes an in-depth look at the processes of the PND and the privacy features associated with those processes.
6. Section 5 presents the findings of the Privacy Impact Assessment and makes recommendations to the IMPACT Programme on how privacy can be addressed within the design of the PND.
7. Section 6 outlines the ongoing review and audit of the effects of the Privacy Impact Assessment.
8. Annex A lists the Bichard Recommendations that the IMPACT Programme is working towards.
9. Annex B details the screening process which was undertaken to decide whether a full scale Privacy Impact Assessment should be undertaken.
10. Annex C lists the organisations that were contacted during the public consultation on Equality, Diversity and Privacy and thanks those organisations and individuals that provided a response to the consultation.
11. Annex D lists the key principles to be applied to ensure the PND is privacy friendly.
12. Annex E details some of the major planned processes of the PND.
13. Annex F lists those persons and organisations who met with the NPIA during the consultation process.

# 1. The IMPACT Programme

## Background

1.1 Following the murders of Jessica Chapman and Holly Wells in August 2002 and the subsequent conviction of Ian Huntley in December 2003, Sir Michael Bichard was tasked by the (then) Home Secretary to lead an independent public inquiry into child protection measures, record keeping, vetting and information sharing in Humberside Police and Cambridgeshire Constabulary.<sup>1</sup>

1.2 The Inquiry Report was published in June 2004 and, amongst other things, identified shortcomings in how the Police Service managed and shared information. For example, Sir Michael noted that, whilst there are national systems such as the Police National Computer (PNC) to which all forces have access, there were “no firm plans for a national IT system” for recording and sharing intelligence. As a result, whilst information like cautions and convictions are available nationally, forces were often unaware of, or found it difficult to access, the intelligence and wider operational information<sup>2</sup> held by other forces.

## The IMPACT Programme

1.3 The IMPACT Programme was established by the Home Office as part of the Government response to Sir Michael’s recommendations. Its objective is to improve the ability of the Police Service to manage and share intelligence and other operational information, to prevent and detect crime and make communities safer. In doing so, the Programme is responsible for implementing those of Sir Michael’s recommendations relating to the management and sharing of information by the Police Service<sup>3</sup>.

1.4 Originally launched under the Police IT Organisation (PITO), the Programme transferred to the Home Office in 2005 and then became part of the National Policing Improvement Agency (NPIA) when the Agency was formally launched on 1 April 2007. The NPIA is a Non-Departmental Public Body of the Home Office, which supports policing in England and Wales and helps forces to improve the way in which they work across a range of policing activities and policy areas<sup>4</sup>.

1.5 IMPACT is judged a ‘mission critical’ programme by the Home Office under Office of Government Commerce (OGC) guidelines. It is a key deliverable for the NPIA and rated as a priority delivery programme by the Association of Chief Police Officers (ACPO) and the Association of Police Authorities (APA).

1.6 The Programme’s current work covers two main strands of activity:

- helping forces to implement the requirements of the statutory Code of Practice and supporting Guidance on the Management of Police Information (MoPI), which provides a national framework for improved and more consistent processes for managing information; and
- delivering a new Police National Database (PND) – an extensive store of police intelligence and other operational information.

---

<sup>1</sup> Further information regarding the Bichard Inquiry and the ongoing implementation work can be found in the reports produced by Sir Michael and the reports that successive Home Secretaries have published on progress against his recommendations. These can be found via [www.webarchive.org.uk/tep/12841.html](http://www.webarchive.org.uk/tep/12841.html) and <http://police.homeoffice.gov.uk/publications/operational-policing/bichard-fourth-progress-report>

<sup>2</sup> The Police Service classes intelligence as operational information that has been evaluated as to its likely accuracy, reliability etc.

<sup>3</sup> The seven recommendations are listed in Annex A

<sup>4</sup> For further information on the NPIA see [www.npia.police.uk](http://www.npia.police.uk)

1.7 The Programme was also responsible for developing the IMPACT Nominal Index (INI) and, until April 2008 when it was transitioned to the NPIA's Operational Services Directorate, for the operation of the INI service. The INI provides a means for an investigating officer in one force to quickly and efficiently establish which other forces might hold information on an individual of interest to their enquiries.

#### The Police National Database

1.8 As the INI is an existing and interim solution<sup>5</sup> that only holds index information, and MoPI is an existing requirement that the Programme is helping forces to implement, the remainder of this report focuses on the Police National Database. In doing so, it recognises that this is not just an IT project; it is helping the Police Service to deliver fundamental business change improvements enabled by IT. In considering privacy, it is therefore necessary to look at both how the IT operates and also how it will be used.

1.9 This report also focuses on Phase 1 of the PND, which will bring together and link information that is currently held only on local systems. Subsequent phases will, subject to agreement of the necessary funding, provide links to information held on a range of existing national systems and will secure the long term future of the existing Police National Computer (PNC). These will be subject to a separate Privacy Impact Assessment.

1.10 The PND will not only address the Government's commitment to implement Sir Michael Bichard's first and ultimately fourth recommendations, it will also provide much wider benefits to the Police Service.

1.11 Unlike the INI which only contains an index of information on people, the PND will hold more detailed information on people (e.g. names, including organisations), objects (e.g. cars), locations (e.g. addresses) and events (e.g. crime reports).

1.12 The Programme has been working closely with the Police Service and other stakeholders to establish and clarify their requirements. As an ongoing project, the exact details of what the system will do, and how it will do it, have yet to be finalised. However, the requirements can be grouped as follows:

- Data Upload and Entry;
- Search and Retrieve;
- Security and Audit;
- Communication;
- Review, Retention and Disposal; and
- System Administration.

1.13 Data Upload and Entry will allow forces to share copies of information that they hold on their local systems with each other and also to enter information onto the PND directly. As well as text, it will be possible to share images, files, maps, video and audio. Users will also be able to create links between records, including where the records belong to different forces.

1.14 Chief Officers will be owners (and data controllers) for the information loaded onto the PND or created on the system by their staff. This will mean that Chief Officers will continue to be responsible for the data, including any links made with other information.

---

<sup>5</sup> The INI will be replaced by the PND.

1.15 Search and Retrieval will allow users to find and view information on the PND. The capabilities will range from simple, structured searches (which would allow a user to find, for example, all records about a particular individual or vehicle) to free text searches (which would allow wider searches for information on the system).

1.16 The PND will help to identify links with other information – e.g. Alan Smith lives at a particular address in Essex and is the keeper of vehicle XYZ 123; this vehicle is also linked with an address in Hampshire.

1.17 It will be possible to transfer data from the PND to other systems that forces use to carry out more sophisticated analyses.

1.18 Security and Audit will help to ensure that the information is kept safe. Only authorised users will be permitted to access the system and they will only be able to view the information that they need. So, for example, access to information about child protection may be restricted to those police staff involved in child protection work.

1.19 As with the INI, all user activity on the PND will be auditable; the details of all transactions on the system and the results generated by those actions will be logged and subject to audit by force or other designated auditors.

1.20 The Communication capabilities will be used for a number of purposes, ranging from very urgent messages (e.g. a terrorist threat) to routine data quality issues (e.g. signalling potential duplicate or incorrect records). “Flags” and “markers” can also be added to records, which will allow users to do such things as provide additional information about a record or register an interest in a record so that they can be notified of any activity relating to it.

1.21 The Review, Retention and Disposal functions will, in accordance with the MoPI requirements, allow forces to re-examine the information they hold, to decide whether they need to retain it and, if not, to dispose of it.

1.22 The PND will introduce further complexities to the review, retention and disposal process. For example, decisions by one force to dispose of one of its records might affect another force, which still needs the information it contains. Decisions about whether to dispose of information may also be affected by information held by another force.

1.23 The PND needs to be flexible to support the variations between forces in policing practice and to adapt to changing policing priorities. To support this flexibility, the PND will be rule-driven with the System Administration function allowing these rules to be set and amended as necessary.

1.24 This function will also allow administrators within each force to manage who within their force can access the system and what they are authorised to do whilst using it.

1.25 The Programme worked with the Police Service to identify their requirements for the system and has gone through the process of selecting a commercial partner to design, build, deploy and run the PND against those requirements. A Contract Notice was published in the Official Journal of the European Union in May 2007. From the 14 consortia that formally responded, the Programme selected three to participate in detailed negotiations. The negotiations are now complete and a contract was awarded to Logica UK at the end of March 2009; the first phase of PND capabilities will commence in 2010.

1.26 The PND is expected to deliver substantial benefits around increased efficiency (where time is saved in obtaining information, or where police operations can be based on better information or information that is obtained more quickly) and effectiveness (such as the prevention and detection of crime).

## **2. Privacy Impact Assessments and why the Programme decided to conduct one**

2.1 In December 2007, the Information Commissioner launched a Privacy Impact Assessment (PIA) handbook, recommending PIAs as good practice for any initiative involving new or significant changes to the processing of personal information.

2.2 The Information Commissioner suggests, in his handbook, what circumstances would trigger the need for a PIA, including:

*'The organisation conducting a project, or some other participating organisation, may appreciate that a proposal has significant implications that should be the subject of investigation'; and*

*'the lead organisation, or perhaps some other participating organisation, considers that a proposal may give rise to public concerns'.*

2.3 More widely, PIAs are extremely helpful in identifying potential privacy issues at an early stage in the development of any new system so that they can be properly considered and addressed. Conducting a PIA at an early stage in a programme helps ensure that data protection and wider privacy requirements can be built in from the start; trying to retro-fit these at a latter stage can cause delays, add significantly to the costs and limit the realisation of benefits.

2.4 The PND creates new information only in the sense that it will help to discover links between existing information and because local force information will be visible to other authorised users of the system; this does not create new operational databases. Whilst many members of the public would expect that forces would routinely share information with each other already, it was recognised that this does raise a number of potential privacy issues.

2.5 The Programme had already been considering these issues and, when the Information Commissioner launched his Privacy Impact Assessment handbook, in December 2007, the Programme realised that there was considerable overlap between the processes that the handbook recommended and the work that the Programme was already undertaking. Whilst PIAs were not compulsory at that time, it was decided, with the endorsement of the Programme's governance structure, to continue that work as part of a PIA.

2.6 In terms of the PND, the purposes of carrying out a PIA were to:

- identify and manage the risks that privacy issues represent to realising the intended benefits of PND;
- generate information to aid decision making and support good governance and business practice around information processing;
- identify any necessary privacy features so these can be designed in at an early stage rather than be subject to costly retro-fitting at a later stage;
- allow privacy considerations to be built into the design from the outset to provide a foundation for a flexible and adaptable system, reducing the cost of future changes and ensuring a longer service life; and
- promote public confidence to maximise the information that people are prepared to disclose to the police and reduce the risks of privacy-related incidents that could undermine public confidence and cause embarrassment to the Police Service, the NPIA or the Government.

### **3. Methodology**

3.1 The handbook published by the Information Commissioner advocates an initial screening to decide whether a PIA is necessary and, if so, whether a full- or small-scale PIA is appropriate. The initial screening involves considering a number of questions that are set out in the handbook.

3.2 The Programme conducted an initial screening in February 2008; the screening questions, and the Programme's answers to them, are included in full at Annex B. These were discussed with members of the Programme and also with the Information Commissioner's Office and the ACPO lead on Data Protection. The results of the initial screening pointed to the need to move on to a full-scale PIA.

3.3 The PIA handbook suggests the following form and structure for a full-scale PIA:

- Preliminary phase – background paper;
- Preparatory phase – stakeholder analysis and consultation strategy;
- Consultation and analysis phase(s) – design issues and privacy problems; design options; privacy impact avoidance measures; privacy impact reduction measures; Privacy-Enhancing Technologies (PETS);
- Documentation phase; and
- Review and audit phase

3.4 As the Programme's work in this area had already commenced and as there was a need to quickly identify any implications for the contract that would be awarded to the chosen supplier of the PND, going back to faithfully follow this structure was not possible or necessary. However, the main elements have all been covered.

3.5 For example, when the handbook was launched, the Programme was already well advanced in its preparations for a full public consultation. This was a requirement of the Equality Impact Assessment that the Programme is also carrying out, but it had already been decided that this consultation should cover privacy as well as equality and diversity.

3.6 As part of the consultation work, the preliminary and preparatory phases had already largely been conducted – the consultation document contained background information on the Programme; an analysis of who the main stakeholders were had been conducted; and a consultation strategy had been decided upon.

3.7 The consultation ran between January and April 2008. It was very broad in nature; asking consultees to identify any privacy issues and how these might be addressed. The consultation document was sent to 47 organisations (Annex C) representing a wide range of views, as well as the 43 England and Wales forces. It was also posted on the NPIA website, on which it received over 800 unique hits – i.e. it was accessed from over 800 different internet addresses.

3.8 Broadly speaking the concerns identified by the respondents can be categorised as concerning access to data, data quality and its interpretation, the sensitivity of some information and the retention of data. However, responses were only received from a narrow range of organisations; only 17 responses were received: 15 were from police forces, police authorities or police related associations and one was from the Information Commissioner's Office. The final one (from the Welsh Language Board) raised equality rather than privacy issues.<sup>6</sup>

3.9 The low number of responses and the narrow range of organisations responding was disappointing; paragraph 3.14 of this document set out our plans for trying to obtain a broader range of views.

3.10 In addition to the consultation a significant amount of internal analysis had also been carried out – the Programme had established a set of key principles broadly based around the Data Protection Principles (see Annex D). The processes that would be enabled by the PND, or that would be needed to support its operation, had also been identified (see Annex E). The Programme then looked at how each of the principles might apply to each of those processes. This helped to identify a large number of detailed requirements; for each of which an assessment was made of whether they would need to be delivered through the design of the IT, or through business processes or a combination of these.

3.11 In carrying out this work, it was the Programme's aim not just to make sure that it was meeting the minimum legal requirements but to minimise, as far as possible given the Programme's aims, the impact on individuals' privacy – i.e. to be "privacy-friendly", not just "privacy-compliant".

3.12 Those of the detailed requirements that involved the IT were fed into the work to set the requirements that the chosen supplier would be required to address in designing, building and operating the system. Those that involved business processes are feeding into the ongoing work to set policies and business rules for the use of the system and the data obtained from it.

3.13 As this work has progressed, there have been a number of relevant developments which have been taken into consideration including:

- The recommendations emerging from the reviews of various incidents involving the loss of personal data;
- The Hannigan review on the procedures for handling data by Government;
- The Home Affairs Committee report on "A Surveillance Society?";
- The "Data Sharing Review" carried out by Richard Thomas and Mark Walport;
- The Review of Criminality Information; and
- The Lords' Constitution Committee report on "A Surveillance Society?"

---

<sup>6</sup> A report on the outcome of the consultation was published on 4 July and can be obtained from [www.npia.police.uk/en/docs/Consultation\\_Response\\_paper\\_v1\\_0.pdf](http://www.npia.police.uk/en/docs/Consultation_Response_paper_v1_0.pdf)

3.14 The outcome of the public consultation and the internal analysis work, and how to progress the PIA, were discussed with the Information Commissioner's Office. It was agreed that we should proceed to the documentation phase. However, we decided we would then use the draft report for a further round of consultation with the hope of obtaining a broader range of input. As well as trying to directly engage some of the organisations that the consultation paper was sent to, we also sought views from the NPIA's own independent advisory panel. Consultation with a number of independent advisory groups or similar bodies was also conducted; a list of those groups is at Annex F.

3.15 Section 6 sets out our plans for formally reviewing and auditing this assessment. However, work will continue to ensure that privacy requirements are fully considered in the detailed design of the PND and the business processes around it.

## 4. Privacy features of the PND and associated processes

4.1 A number of features of the PND itself will help to make it privacy friendly:

- there will be safeguards to ensure that the system is only accessible by authorised, trained users;
- users will only be able to access the sorts of information and facilities that they need to do their job;
- all use of the system will be logged and subject to audit;
- the PND capabilities will be designed with full consideration of privacy requirements;
- rules for the use of the system, and of any information obtained from it, will be set. These will include that the system and data must only be used for policing purposes<sup>7</sup>.

### Safeguarding access to the system

4.2 The PND will be able to hold information rated up to CONFIDENTIAL according to the Government Protective Marking Scheme (GPMS)<sup>8</sup>. Although not all data held on the PND will attract a protective marking as high as CONFIDENTIAL, all data will be protected as if it were at this level according to the Government guidelines using means approved by national accreditors. Within police forces, data will also be protected at the appropriate level.

4.3 In Phase 1, the PND will only be available to policing organisations over the secure Police National Network. Initially, this means the 43 forces in England and Wales, the eight Scottish forces, British Transport Police, Police Service of Northern Ireland and the Ministry of Defence Police and Guarding Agency.

4.4 Another NPIA programme - Identity and Access Management (IAM)- will help ensure that only authorised users can access the system. IAM will improve access to national police data services, not just the PND. It will make it both easier and more secure by using a single digital identity utilising smartcard technology. For the PND, this will mean that it will not be necessary to rely on less secure user passwords that can be compromised or shared, and that users will be identifiable whether they access the system directly or via a local interface<sup>9</sup>. IAM will also help to ensure that any use of the PND can be traced through a rigorous and secure auditing process (see paragraphs 4.6 - 4.12).

### Safeguarding access to the data and PND capabilities

4.5 IAM will also support "Role Based Access Controls" which will ensure that users only have access to capabilities and information that they need for their business role. For example, access to child protection information is likely to be limited to those involved in child protection work.

---

<sup>7</sup> Defined in the MoPI Code of Practice as: "protecting life and property; preserving order; preventing the commission of offences; bringing offenders to justice; and any duty or responsibility of the police arising from common or statute law".

<sup>8</sup> The GPMS is a system for protecting information. It has 4 main levels of protective marking. In order of the amount of harm that could be caused by unauthorised disclosure, these are: RESTRICTED, CONFIDENTIAL, SECRET and TOP-SECRET. A fifth marking – PROTECT – is also sometimes used; it sits below RESTRICTED.

<sup>9</sup> As well as accessing the PND directly, it will be possible for forces to link their systems to the PND and access PND data through those.

## Auditing use of the system

4.6 In addition to securing access to the system and to the data within the system, the PND will have extensive auditing systems, helping to deter misuse and, where misuse does happen, helping to identify and provide evidence against those individuals involved.

4.7 All activity within the PND will be logged; this will include all upload of data, both manual and automatic feeds; searches and other data retrieval; reviews and disposals; and administrative activities. These will record who did what, when and what results were obtained.

4.8 Every time they search the system, users will also have to enter information saying why they were doing so and, where appropriate, on whose behalf. This information will also be logged

4.9 In addition to identifying misuse of access rights, the audit service will help to identify attacks on the PND from external sources and from attackers attempting to bypass the system access controls from within.

4.10 The audit log will be used strictly for the purposes of:

- proving the integrity of the transactional data to support evidential disclosure of fact-based data on PND; and
- monitoring the PND for improper use, including analysing patterns of usage over a period of time.

4.11 The log will only be available to force auditors, who will only normally be able to see audit data relating to their force. Auditors will carry out both reactive (i.e. investigating where misuse is suspected) and proactive audits (i.e. random sampling of all activities to check for misuse).

4.12 The activities of auditors on PND will also be logged and subject to audit.

4.13 The Programme will be seeking feedback from auditors on any problems identified so that consideration can be given to the need to strengthen the controls, either through the IT or business processes.

## The design of the PND capabilities

4.14 The work described in paragraph 3.10 has led to some detailed requirements for the design and use of the PND. Trying to cover all here would make this document too long. However, a few examples are particularly worth outlining.

### *Data export*

4.15 It is an essential part of the National Intelligence Model (NIM)<sup>10</sup> that the Police Service has the ability to not just search and link the data that will be on the PND, but also to be able to analyse it using intelligence tools. Forces already use a number of different analytical products, therefore providing an analytical capability within the PND would involve additional costs to duplicate capabilities that already exist. Instead, it was decided to provide a capability to allow data to be exported from the PND for analysis by forces using their own local tools. There is also a need to export particular data items – for example, producing electronic or hard copies of individually selected records that a user needs.

---

<sup>10</sup> Full details of the National Intelligence Model can be found at <http://police.homeoffice.gov.uk/publications/operational-policing/nim-introduction>

4.16 A number of measures are being considered to protect the export processes and any information that has been exported. These include:

- limiting the ability to export large amounts of information
- senior management authorisation of bulk exports
- anonymisation / pseudo-anonymisation of information wherever possible
- business rules regarding the use and security of the information
- encryption of the information
- ensuring the information carries appropriate protective markings
- “watermarking” (to show, for example, who exported the information and when it was exported).

4.17 Further work is continuing in the area of information export, concentrating on:

- the controls over who will be authorised to export information
- how export of information would be monitored
- the physical security of the transmission of information between the PND and the local intelligence tool
- the security of the information whilst held on the local intelligence tool
- how access and other controls provided by the PND will be maintained once the information leaves the PND
- how requirements to keep information up-to-date and to not keep information longer than is necessary can be met once it has been exported from the PND

#### *Data quality and consistency*

4.18 Data quality and consistency are important aspects of privacy. They are also necessary to ensure that the PND is an effective tool and delivers a system that meets the needs of the Police Service; data quality has been identified as one of the main potential barriers to the successful implementation of the PND. Data which are incomplete, inconsistent, not meaningful or misinterpreted due to the different ways forces manage their information can lead to poor decisions, wasted time or missed opportunities.

4.19 The work forces are doing to implement the Management of Police Information requirements will help to ensure that data is better collected and recorded, analysed, reviewed and, where no longer needed, disposed of.

4.20 The Programme is also assisting forces in their efforts to ensure that their data is consistent and of a known quality. To achieve this, we are working with forces to help them develop a national standard which data must conform to. Monitoring and quantifying the quality of information uploaded by forces will inform the design of the PND from a data quality perspective. Feeding back information to forces where the data do not meet the standards will help them to drive up quality.

4.21 In the run up to deployment of the PND, we have been working with forces since 2007 to discover and address data quality issues. Central data profiling is a process which is enabling the Police Service to assess data consistency against the IMPACT data quality standards. A central data profiling environment is available to allow data quality issues to be uncovered. These can often be dealt with locally (for example via the force MoPI project board). However, where appropriate issues can also be raised at a national level via bodies such as ACPO's Information Management Business Area or via the PND project for clarification of the data quality standards and the PND requirements.

*Ensuring data are up-to-date, accurate, relevant, not excessive, adequate and used fairly*

4.22 Ensuring that data are up-to-date, accurate, relevant, not excessive, adequate and used fairly are all elements of the 8 data protection principles. However, reviewing each item of information against these criteria before placing it on the PND is not practicable – we anticipate there will be at least 70 million records containing personal information. In addition, deciding what is fair, relevant, not excessive and so on depends on the circumstances in which the data will be used, and whether something is accurate and up-to-date can quickly change.

4.23 We therefore plan to place the responsibility on users of the system to consider, within the context of the enquiry they are dealing with, whether these criteria are met. In doing so, they will need to consider whether it is necessary to contact the force that originally obtained the information to check whether it is still up-to-date and accurate.

4.24 Where information is discovered which appears to be out-of-date, inaccurate, not relevant or excessive there will be facilities to flag the relevant record so that the originating force can investigate and take the necessary steps to rectify any issues.

*Victim and witness information*

4.25 The question of whether information about victims of crime and witnesses should be included in the PND has raised considerable debate. Ultimately, the decision must rest on whether it is necessary and proportionate to do so and the Programme has consistently taken the position that it must be for the Service to assess this – it is best placed to make such judgements, and it will be for the Service to justify any such sharing.

4.26 The need for, and value of, sharing such information for policing purposes has been considered alongside the potential implications for the privacy of the individual concerned. It has been decided that there is no legal justification for sharing witness records on the PND, and that victim records should only be shared where justified on a case-by-case basis<sup>11</sup>. Where victim information is loaded, it will be subject to additional protections. For example, where users want to include victims in a search they are carrying out, they will be required to specifically justify this for the audit log.

4.27 This position is based on discussions both within the Police Service and with the Information Commissioner.

4.28 Alongside work undertaken by the Programme to arrive at this definition, ACPO (Crime and Intelligence) have been reviewing the ACPO position on sharing victim information. This work has identified that a potential consensus has emerged that routine sharing of victim information could only be fully justified where there was a demonstrable link to the 'safeguarding agenda'. The outcome of this work will be taken to ACPO Cabinet for endorsement. The Programme will provide assistance to this process. It is anticipated that the final ACPO decision will be compatible with the working definition of case by case adopted by the BDA.

4.29 It is recognised that victim and witness information may also be contained within records about crimes, suspects, offenders and others. Where possible, victim and witness information should be removed from such records but it is accepted that this will not always be practical, particularly where the information is within free text fields. The Programme is continuing its consideration of this issue.

---

<sup>11</sup> At the meeting of the Business Design Authority (BDA) on 26<sup>th</sup> March 2009 the BDA was asked to give direction to the Programme on what is meant by sharing victim information on a case by case basis.

After considering a number of options the BDA advised that the IMPACT Programme should use the following definition of case by case when sharing victim information:

*'Sharing victim information on a case by case basis' means 'loading victim information only from those offences (crimes) listed in Schedules 3 and 5 of the Sexual Offences Act 2003, and then allowing unrestricted searching of that information'.*

This will now be used as a working definition for the PND by forces, the Programme and the supplier. This working definition has been taken through the Programme governance process and duly endorsed.

In reaching this definition the following was taken into account:

- Offences in schedule 3 and 5 of the Sexual Offences Act 2003 are those offences for which it is possible for a court to grant a sexual offences prevention order;
- The offences include serious crimes of violence (e.g. murder, kidnapping, wounding with intent to cause Grievous Bodily Harm etc) and sexual offences; and
- All searches on PND (including searches of victim records from these specific crimes) are subject to information assurance controls (e.g. PND will be based in a confidential environment, users will be trained, and access will be subject to identity access management, system rules, business rules, role based access controls and audit).

### *Medical and health information*

4.30 There is a necessity for some information about people's health to be placed on the PND so that the Service can, for example, provide adequate care for individuals who are placed in custody or to help safeguard their officers. There will be restrictions on who can access such information and how it can be used.

### *Retention and up-dating of data uploaded to PND*

4.31 The PND will contain information which each force has agreed to load to the system from their own data stores. The information provided by each force will be updated on at least a daily basis, keeping the data as up-to-date as possible.

4.32 When a force disposes of data from its local system, the copy of that data held on the PND will also be disposed of. (Any copy of that information held in audit logs will normally be retained but only for use for auditing purposes.)

### *Openness and transparency*

4.33 The Data Protection Act requires, subject to certain exemptions, that data subjects be told what information is held on them and how it is used. We will be working with the Service and the Information Commissioner to consider how best to meet this requirement. It will often not be possible to tell subjects exactly what data is held on them or exactly how it is being used as this could compromise the prevention and detection of crime. It may sometimes not even be possible to tell individuals whether any information is held on them. However, we are looking at ways of making sure that those who come into contact with the police for operational reasons know, in general terms, that information about them may be shared with other policing agencies.

4.34 More generally, we aim to be as open and transparent as possible about the PND.

4.35 Chief Officers are acting as "data controllers in common" for the information on the PND. As such, it has been decided that they all "hold" all the information on the PND that they can access. In responding to subject access requests<sup>12</sup> they must therefore consider all the information on the PND, not just the information provided by their force.

### Business rules

4.36 Whilst the PND itself will provide a high level of protection for the data, the need for rules around how the system and any information obtained from it are used has also been recognised. The Home Office has agreed these will take the form of a statutory code of practice with attendant more detailed guidance. Chief Officers are legally required to have regard to such codes of practice.

---

<sup>12</sup> Subject to certain exemptions, the Data Protection Act gives data subjects the right of access to details of the information held on them and how it is used.

4.37 The guidance will address issues including:

- The purpose of the PND and any restrictions on its use;
- Some general concepts, such as the responsibilities of Chief Officers (as “Data Controllers in common”), the need to ensure the system is used in a way that is non-discriminatory, the security of the system and who will have access;
- Loading data – including the principles for what information to send / not send, data quality and interpretation, how the requirements relating to the review, retention and disposal of police information will apply to the PND, how the linking of information will work;
- Using the PND – including searching, administering and auditing, and the vetting and training of users;
- Using the information from the PND – responsibilities for ensuring it is fair, necessary, proportionate, accurate and up-to-date; ensuring information obtained from the system is managed appropriately; disclosure of the information to other agencies; and
- Other matters such as dealing with subject access requests.

4.38 The high level strategy in the form of a code of practice will be published. We also plan to publish the guidance though some elements may have to be withheld as they could prove useful to criminals in committing crimes and avoiding detection.

## **5. Findings and recommendations**

5.1 We are working actively, and will continue to do so, to ensure that the PND and the way that it is used are as privacy-friendly as possible.

5.2 Further work, including the planned ongoing consultations, will be carried out to ensure the potential impacts on privacy are identified and fully considered in designing, implementing and using the system, and using the data obtained from it.

5.3 The Programme can address privacy in the way the PND is designed, the way the supplier operates, in establishing the necessary business rules and in helping to design suitable training. However, forces also have a key part to play in ensuring that they use the system, and the data obtained from it, appropriately. This is ultimately the responsibility of the Chief Officer. However, the Programme will be asking forces to:

- (i) abide as fully as possible with the business rules, which will be associated with a statutory code of practice;
- (ii) review their existing policies and practices to ensure they take account of the potential impacts on privacy;
- (iii) ensure they have sufficient auditing resources in place to properly audit the use of the PND and that appropriate action is taken when any misuse is identified; and
- (iv) participate in the data profiling process to assist in raising the quality of the data they intend to share through the PND.

## **6. Review and audit**

6.1 The purpose of “Review and audit phase” of a PIA are to check whether the actual impacts on privacy are those that were anticipated and that the actions that emerged from the PIA have been taken forward and are having the expected effects. Where either is not the case, it allows further action to be taken to assess the impacts and to take whatever extra action is needed.

6.2 Impact on privacy will be something that the Programme continues to consider at all stages as our work progresses. We anticipate carrying out more formal reviews at a number of key stages. For example, we plan to roll out the system in waves based on business priorities, initially to a small number of “early adopter forces” – the initial deployment of wave 1 to the early adopters would seem a suitable point to carry out a review. Another after the system has been in full use for several months is also planned.

## **The seven Bichard Inquiry recommendations that the IMPACT Programme is addressing**

### **Recommendation 1**

A national IT system for England and Wales to support police intelligence should be introduced as a matter of urgency. The Home Office should take the lead and report by December 2004 with clear targets for implementation.

### **Recommendation 2**

The PLX system, which flags that intelligence is held about someone by particular forces, should be introduced in England and Wales by 2005.

### **Recommendation 4**

Investment should be made available by Government to secure the PNC's medium and long-term future, given its importance to intelligence-led policing and to the criminal justice system as a whole. I note that PITO has begun this work.

### **Recommendation 8**

A Code of Practice should be produced covering record creation, review, retention, deletion and information sharing. This should be made under the Police Reform Act 2002 and needs to be clear, concise and practical. It should supersede existing guidance.

### **Recommendation 9**

The Code of Practice must clearly set out the key principles of good information management (capture, review, retention, deletion and sharing), having regard to policing purposes, the rights of the individual and the law.

### **Recommendation 10**

The Code of Practice must set out the standards to be met in terms of systems (including IT) accountability, training, resources and audit. These standards should be capable of monitoring both within forces and by HMIC and should fit within the Police Performance Assessment Framework.

### **Recommendation 11**

The Code of Practice should have particular regard to the factors to be considered when reviewing the retention or deletion of intelligence in cases of sexual offences.

## PIA screening questions and answers

### Introduction and purpose

The first stage of the PIA process is a set of screening questions, the answers to which determine what further work is needed. This annex sets out our initial responses to those questions, which have been discussed with the Information Commissioner's Office.

The answers and analysis refer primarily to our expectations of what Phase 1 of the PND will deliver.

### Step 1 – Criteria for a Full-Scale PIA

*Do the characteristics of the project indicate that a full scale PIA is needed?*

#### Technology

*1 Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?*

**Yes.** The PND will not involve the collection of any new information. However, the PND will be applying new or additional technologies in the way it brings together and links existing information, and in the capabilities it will offer for searching and using that information. These do have potential for privacy intrusion.

An objective of PND phase 1 is that it will provide a single source of the operational information and intelligence that is currently available across the 43 local force systems. This would provide forces with the ability to quickly and efficiently find and access intelligence and other operational information on people, objects, locations and events from across the Service.

Although the system will be able to suggest associations between information where it believes there are links, it will be for police personnel to confirm, and be responsible for, any associations.

The system will not provide any data mining, pattern analysis or other sophisticated intelligence capability. Forces will instead be able to export data for analysis on their own intelligence systems.

Support for additional device types, such as PDAs, smartphones or Blackberries, and the provision of alternative delivery mechanisms, such as Airwave, are not currently in scope for Phase 1 of the PND, but may be considered in later phases, by which time it is anticipated that the Identity and Access Management (IAM) arrangements will be fully functional. It is possible, however, that forces may decide to provide support for such delivery mechanisms themselves. The level and quantity of information accessible through such channels is expected to be more limited (name, address, date of birth, possibly a photograph, an indication of the number of records held on the individual, PNC identifier and vehicle details).

#### Identity

*2 Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?*

**Yes.** For persons who are the subjects of police records, there will be a new, unique PND identifier. It is planned that where information from different forces about the same individual can be linked, it will be brought together under this identifier.

For users of the system, the PND will be utilising the work that is currently being undertaken by the Identity and Access Management (IAM) programme within NPIA. It will involve users having a single digital identity utilising smartcard technology and will deliver a framework that provides identification and authentication services for national police data services.

IAM aims to ensure information is being accessed by the right people, whether via direct access to the PND or via local systems that have an interface with the PND. It will help ensure that forces are satisfied that persons making requests for information are who they say they are, and that they have a legitimate business need to access the information held by other forces.

Smartcards and smart card readers are currently the preferred option of secure access by the IAM programme. All users who require IAM will be issued smart cards and smart card readers. IAM is also exploring the use of RFID tags and biometrics.

*3 Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?*

**Yes.** Forces will be sharing personal and sensitive personal information about individuals which previously would not have been visible to other forces. In most cases, it will not be possible to anonymise or pseudo-anonymise the information.

If forces do not manage their information and intelligence correctly, and do not comply with the relevant legislation and other requirements, then there are a number of individuals that are at risk of having their anonymity inappropriately disclosed. Particular issues include:

- Victims – discussions are ongoing within the Police Service as to the extent to which victim information can be shared, for what purpose and how it can best be protected. Some victims may have a legitimate expectation that their personal information would not be widely shared;
- Details of informants are at risk of being disclosed if data is shared contrary to the handling rules that form part of the National Intelligence Model. The ability of the PND to link information could also help to identify where information might have come from, potentially placing the individuals who provided it at risk;
- In some cases, police officers may need to keep their identity safeguarded and provide information anonymously - for example, undercover officers, test purchase officers, and officers involved in combating terrorism.

### Multiple Organisations

*4 Does the project involve multiple organisations, whether they are government agencies (e.g. in 'joined-up government' initiatives) or private sector organisations (e.g. as outsourced service providers or as 'business partners')?*

**Yes.** The PND will provide for the sharing of information and intelligence on a national scale, during Phase 1 the information will be shared between the 43 England and Wales police forces, the 8 Scottish forces, the Police Service of Northern Ireland, British Transport Police, Ministry of Defence Police and Guarding Agency.

In addition the following government agencies and local authorities are key stakeholders of the Programme:

- Home Office
- Ministry of Justice
- Association of Chief Police Officers
- Association of Police Authorities
- Other policing agencies (primarily)

The public is also a stakeholder – both those who are the subjects of police records and also more widely as the system will help to prevent and detect crime. It is also being delivered using public money.

The procurement phase for a final supplier of the PND is ongoing. Three private sector consortia have been selected for detailed negotiations with a view to signing a contract with the successful supplier in Spring 2009.

## Data

*5 Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals?*

**Yes.** By its nature, the Programme does require that the ways in which personal data will be handled will be significantly changed. Whilst many individuals might think that policing information is already shared across the Service, it is likely that others would be concerned to know that information about them is being made more widely available, especially in regard to the current interest in Government data losses and the 'surveillance society.'

The data held on the PND will include 'sensitive personal data' as defined by Section 2 of the Data Protection Act. This could include, but is not limited to:

- Racial and ethnic origin;
- Political opinions;
- Religious beliefs;
- Sexual life;
- Offences; and
- Court proceedings.

Such data will require special protections including rules on how it can be used.

It is not anticipated that categories of data which are likely to give rise to identity theft, or financial data, will be available on the PND.

6 *Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database? and*

7 *Does the project involve new or significantly changed handling of personal data about a large number of individuals?*

**Yes to both.** It will pull together, on a national scale, information and intelligence regarding persons of interest to the police. This increases the possibility that there will be significant amount of data with regard to certain individuals.

The PND will pull together information and intelligence on the criminal population of England and Wales.

The IMPACT Nominal Index currently contains nearly 64 million records – whilst there is some duplication and some individuals will have multiple records on the INI, this shows that the police hold significant quantities of information about a large number of individuals.

8 *Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?*

**Yes.** The PND will facilitate the inter-linking, cross referencing and matching of personal data from around 300 systems across the Police Service and other UK policing agencies.

#### Exemptions and exceptions

9 *Does the project relate to data processing, which is in any way exempt from legislative privacy protections?*

**Partly.** Whilst the processing will be subject to the protections afforded by the Data Protection and Human Rights Acts and other relevant legislation, some of the processing may, on a case-by-case basis, be exempt from some aspects of the legislative privacy protections under Section 29 of the Data Protection Act (which covers the use of personal data for crime and taxation purposes).

10 *Does the project's justification include significant contributions to public security measures?*

**Yes.** The justification for, and a clear objective of, the creation of a PND is to make the public safer by improving the ability of the Police Service to manage and share operational information to prevent and detect crime. Some of the high level strategic benefits identified aligned to policing functions are improved performance in the following areas:

- safeguarding children and vulnerable adults;
- countering terrorism;
- proactive crime prevention and disruption, including serious and organised crime;
- public, officer and staff safety; and
- detections (reactive criminal investigation process).

*11 Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?*

**No.** In Phase 1, access to the data is expected to be restricted to UK police forces or other public sector policing agencies. Even in the longer term, the PND is very unlikely to be directly involved in any systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulations.

## **Conclusion**

The characteristics of the project indicate that a full scale Privacy Impact Assessment is required. It was not therefore necessary to carry out Step 2 of the screening process, as this looks at whether a reduced scale PIA is needed. It only applies where a full scale PIA is not needed.

The next stage of the screening process is to conduct Steps 3 and 4, which respectively assess whether privacy law and Data Protection Act compliance checks are required.

### **Step 3 – Is privacy law compliance checking necessary?<sup>13</sup>**

#### Are any of the activities subject to any form of privacy law?

*Does the project involve any activities (including any data handling) that are subject to privacy or related provisions of any statute or other forms of regulation, other than the Data Protection Act?*

Yes. The development of the PND does include data handling activities that are subject to further statutory provisions and regulation, other than the Data Protection Act.

Consideration of the following acts / regulations will be required in the development of the PND and the policy / guidance regarding how the PND, and the data on it, should be used.

#### **1. Human Rights Act 1998**

Article 8<sup>14</sup> is particularly relevant to the development of the PND. The PND will link information and intelligence held on local police systems, onto a national system. Potentially, this will draw together information regarding individuals held by one force, which other forces did not previously know existed, creating a wider basis of intelligence. It is imperative that Article 8 of the HRA is considered at all times both during the development of the PND and in establishing the business regime such as access rights. Currently, it is anticipated that access rights will be restricted dependant upon the seniority of the officer or civilian user and the area of police work in which they operate.

Article 14<sup>15</sup> must also be considered in the context of the information and intelligence that is collated, how it is collected and stored, and how the information is used and shared with others and for what purposes. For example, Article 14 would apply in situations whereby the sharing of information with another country, could lead to an individual being discriminated against due to that country's laws and / or culture.

#### **2. Police Act 1997 – Part V**

Part V of the 1997 Act creates a statutory scheme for access by prospective employers to the criminal records and, in limited circumstances, other information held by the police relating to potential employees. It places a duty on Chief Officers of police to provide information, for standard Criminal Records Bureau (CRB) checks, from 'central records' which refers to conviction and caution information held on the Police National Computer. In the case of enhanced CRB checks, Chief Officers are

---

<sup>13</sup> Whilst a PIA is best commenced at an early stage of the overall project, compliance checking activities are usually conducted once a fairly mature stage of business process design has been reached. The process can begin early, but cannot be finalised until late in the project life-cycle, when the design is complete.

#### <sup>14</sup> **Article 8 Right to respect for private and family life**

Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

#### <sup>15</sup> **Article 14 Prohibition of discrimination**

The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

requested to provide any information in their possession that may be relevant when an employer makes consideration of an applicant's suitability for a position. Such non conviction information is recorded within individual police forces databases and, as such, is likely to be placed on the PND.

### **3. The Regulation of Investigatory Powers Act 2000**

The Regulation of Investigatory Powers Act 2000 (RIPA), provides the legal basis through which the privacy rights of an individual (created under the Human Rights Act 1998), can be lawfully breached. RIPA allows for different levels of intrusiveness, for example the interception of a telephone call which requires ministerial authority, through to looking at telephone records. RIPA also covers varying levels of surveillance, intercepting electronic traffic and communications data.

The nature of some of the data collected by forces will require that there are strict guidelines to forces as to how information and intelligence gathered under RIPA is to be managed, including placing the information onto the PND and how to sanitise it appropriately. Forces will be legally obliged to ensure that the data that they enter onto the PND, which has been collected under RIPA, does not conflict with the terms of RIPA. It will be necessary that all RIPA information and intelligence be subjected to the 5x5x5 Information / Intelligence Report as outlined under the Guidance on the Management of Police Information, prior to being placed upon the PND. If one force requires further information than that available on the PND, then the appropriate force will need to be contacted.

It is recommended that further work regarding RIPA and the entering of information and intelligence onto the PND is undertaken as part of the business change work.

### **4. Lawful Business Practice Regulations 2000**

The Lawful Business Practice Regulations 2000 are relevant to the information that is stored and accessed upon the PND. There is potential that intercepted communications information and intelligence will be stored upon the PND. To maintain the integrity of the system, persons inputting the intercepted information should ensure that the material was legally obtained by following the regulations which are summarised below:

*The interception has to be by or with the consent of a person carrying on a business (which includes the activities of government departments, public authorities and others exercising statutory functions) for purposes relevant to that person's business and using that business's own telecommunication system.*

*Interceptions are authorised for:*

- *monitoring or recording communications;*
- *to establish the existence of facts, to ascertain compliance with the regulatory or self-regulatory practices or procedures or to ascertain or demonstrate standards which are or ought to be achieved (quality control and training);*
- *in the interests of national security (in which case only certain specified public officials may make the interception);*
- *to prevent or detect crime;*
- *to investigate or detect unauthorised use of telecommunication systems or,*
- *to secure, or as an inherent part of, effective system operation;*
- *monitoring received communications to determine whether they are business or personal communications;*
- *monitoring communications made to anonymous telephone helplines.*

*Interceptions are authorised only if the controller of the telecommunications system on which they are affected has made all reasonable efforts to inform potential users that interceptions may be made.*

*The Regulations do not authorise interceptions to which the persons making and receiving the communications have consented as these are not prohibited.*

Current policing guidelines regarding the use and storage of intercepted material *to prevent and detect crime* must be reviewed to ensure that police forces are compliant with the regulations when using the PND.

## **5. The Privacy and Electronic Communications Regulations 2003**

These Regulations are concerned with the regulating of direct and indirect marketing through electronic means. This would not be relevant to the PND as the PND will not be involved in any such marketing, neither will it be sending out e-mails to individuals to gather support for charitable organisations and / or political parties.

## **6. The Data Retention (EC Directive) Regulations 2007**

The Regulations are concerned with the providers of public electronic communications services or networks ('providers') to retain certain categories of data. The PND will not be providing a public communications service or network, as it will only be available to individuals / bodies that are lawfully entitled to access the information, and subject to specific access rights.

## **7. Common Law of Confidentiality**

Traditionally, the English common law has protected an individual's right to expect that personal information about him or her will be kept confidential. Information will be protected if it has "the necessary quality of confidence about it" and has been provided or obtained in circumstances imparting an obligation of confidence. For example, information given to a doctor, social worker or lawyer would normally be considered to have this quality of confidence, but a conversation with a friend would not. A duty of confidentiality may also arise as a result of a contract where one party agrees to keep confidential information provided by the other party.

A court can prevent the disclosure of confidential information by injunction and, where appropriate, award damages if unlawful disclosure has been made.

The law imposes a 'duty of confidence' whenever a person receives information they know or ought to know is fairly and reasonably regarded as confidential. The confidentiality can either be **implicit** or **explicit**:

**Implicit** – Where the nature of the information and circumstances imply that a person should keep the information confidential, there is **an implied duty of confidence**. In particular, where disclosure of that information could cause substantial harm or offence, or it is self-evidently confidential, or implicitly confidential by custom and practice e.g. relationship between employee and employer or client and solicitor or doctor and patient.

There will often be an implicit duty of confidence where a public authority has statutory powers to obtain information.

**Explicit** – There is a duty of confidentiality where a person or organisation **expressly agrees** to keep information confidential, provided the information has the necessary **quality of confidence** e.g. confidentiality clauses in contracts and agreements.

There are two main exceptions to the duty of confidence. Firstly, public interest can override the duty. For example, a psychiatrist could pass on information about a patient to the police if it was felt that the patient was a danger to third parties. Secondly, disclosure of confidential information may be permitted or required by statute or court order.

Information and intelligence gathered prior to, and following the implementation of the PND, could be subject to the common law of confidentiality. Policy should be considered as to how, if necessary, the information imparted to an officer can be used, and how an individual is informed (at point of original contact, or prior to the use of the information) about how their information will be processed. Although this situation currently exists, and works on a smaller scale due to local force systems, it is necessary to understand what changes may occur to the use of this information if it is to be made available on a national scale.

## **8. Tort of Privacy**

Although there is no legal tort of privacy in the United Kingdom, there is evidence to suggest that it is emerging in case law. With regard to this, the progression of the PND should look at recent cases in which privacy is cited, to understand what future provisions may need to be built into the system.

Tort law is a branch of civil law, and is defined as a legal wrong. In civil law the dispute is typically between private parties. However, governments can also be sued. An action in tort is defined by Her Majesty's Court Service as *'a claim for damages to compensate the claimant for harm suffered. Such claims arise from cases of personal injury, breach of contract and damage to personal reputation. As well as damages, remedies include an injunction to prevent harm occurring again.'*

## **9. Industry Standards – BS ISO/IEC 17799:2005 Information Security Standard**

BS ISO/IEC 17799:2005 is an information security standard. The standard requires that organisations establish a set of business controls for information security and promotes a common standard on best practice.

The standard is consistent with the OECD (Organisation for Economic Cooperation and Development) guidelines on privacy, information security and cryptography. BS ISO/IEC 17799:2005 best practice controls are described in a way that can be implemented in a variety of legal and cultural environments. For example, BS ISO/IEC 17799 does not prescribe particular solutions to protection of IP or personal data privacy; it does, however, specify the security objectives that need to be achieved whatever the implementation circumstances.

To obtain the standard is not a mandatory international certification scheme; however, there are clear benefits in a common framework for information security management, particularly when drawing together information and intelligence from a variety of sources from across 43 police forces.

The PND should aim to achieve the BS ISO/IEC 17799:2005 information security standard, as this will promote confidence within the system both internally within the NPIA and its partner agencies, within the Police Service and the public. However, it is currently unclear at this stage what would be required for the certification to be granted to the IMPACT Programme for the PND. There is potential to ensure that developing the system towards achieving, and maintaining the standard as it evolves in the future, is made into a contractual obligation upon the final supplier.

Currently a certificate will normally be valid for three years, subject to satisfactory maintenance of the system. The system will be checked by the certificate awarding body at least annually during surveillance visits. Subject to the outcome of the surveillance visits, certification will typically be renewed for a further three years. With regard to the confidential and national security nature of the PND, this raises the legal question as to whether the accreditation body would be allowed access to the system, thereby potentially having sight of confidential information and intelligence.

In the UK, the United Kingdom Accreditation Service (UKAS), operating under a Memorandum of Understanding from the Department of Trade and Industry, accredits the competence of certification bodies to performance services in the areas of product and management system approval. It is strongly recommended that the potential of the PND in achieving accreditation for the standard is further explored with UKAS.

It is recommended that the potential of the PND in achieving the standard is investigated in greater detail within the main Privacy Impact Assessment.

## **10. The sharing of information on children and young people**

The sharing of information on the PND must give regard to the guidance (*Information Sharing: Practitioners' guide*), and advice that the Department for Children, Schools and Families (DCSF) provides for the sharing of information relating to children and young people.

The Guidance provided by DCSF, as part of the Every Child Matters scheme, is non-statutory guidance; however, it provides strong advice as to how and when personal information regarding children and young people can and should be shared.

Police personnel should regard the guidance when processing information about children and young people, and when sharing that information. In particular, care must be taken in the future when information or intelligence is placed on the PND, potentially becoming accessible to Child Protection Unit officers on a national scale.

The DCSF Guidance recommends that consent is sought for the sharing of information either from the child / young person if they comprehend and are able to make a sound decision, or from a responsible adult. Information concerning the child / young person can be shared without consent if it is believed to be in the public interest that the information is shared, or that the child / young person 'may be suffering or may be at risk of suffering serious harm.'

Information sharing may also be necessary if there is a statutory purpose to share the information, or if the information is the subject of a court order.

Further investigation into the sharing of information on children / young people on a national scale is required for the purposes of the sharing and storing of information on the PND.

## **11. Police and Criminal Evidence Act (PACE) 1984**

An aim of PACE is to establish a balance of powers between the police service and the public. PACE provides a legislative framework for the powers of the police to combat crime, and also provides codes of practice for the exercise of those powers.

Any person with a duty of investigating offences or charging offenders is required to follow the provisions of the PACE codes as far as practical and relevant.

Development and implementation of the PND must ensure that due regard is given to PACE, particularly in relation to the retention and storage of information and intelligence on the system, and the manner in which that data is utilised by authorised users of the PND.

The PACE Codes of Practice, which the development and implementation of the PND should have due regard to and must consider further, are outlined below.

- PACE Code A – deals with the exercise by police officers of statutory powers to search a person or a vehicle without first making an arrest. It also deals with the need for a police officer to make a record of such a stop or encounter.
- PACE Code B – deals with police powers to search premises and to seize and retain property found on premises and persons.
- PACE Code C – sets out the requirements for the detention, treatment and questioning of people in police custody by police officers.
- PACE Code D – concerns the main methods used by the police to identify people in connection with the investigation of offences and the keeping of accurate and reliable criminal records.
- PACE Code E – deals with the tape recoding of interviews with suspects in the police station.
- PACE Code F – deals with the visual recording with sound of interviews with suspects.
- PACE Code G – deals with statutory powers of arrest; and
- PACE Code H – deals with the detention of terrorism suspects.

It is strongly recommended that further work is undertaken with regard to the requirements of PACE in relation to the information that the PND will retain, including how data are recorded and inputted, how the information is used and for what purposes, and who will have access. This must cover not just the transactional data (i.e. about suspects, offenders, crimes) but also the audit logs as these could become evidence in cases of misuse of the PND. It is imperative that PACE forms an integral part of the understanding of how the PND will be developed and implemented as it forms the legislative framework for policing powers.

## **12. Criminal Procedures and Investigations Act 1996**

Further work is required as to how the type of information and intelligence on the PND (again including audit logs) is collated and stored to ensure that *the information which is obtained in the course of a criminal investigation and may be relevant to the investigation* is correctly retained for the purposes of the Criminal Procedures and Investigations Act 1996. A failure to ensure this is managed correctly for the PND could result in errors occurring at a later stage in the criminal justice system.

## **13. Computer Misuse Act 1990**

The Computer Misuse Act covers three offences:

- unauthorised access to computer material (for example out of curiosity);
- unauthorised access with intent to facilitate the commission of a crime (for example fraud or blackmail); and
- unauthorised modification of computer material (for example fraud or blackmail).

The Computer Misuse Act relates in two main ways to the development and implementation of the PND, and the information and intelligence that is held, or made accessible, via the system.

Primarily the PND must be a secure system with multiple security levels / firewalls that strongly inhibit and deter misuse of the system both by authorised users or external threats. The PND requires a notification function whereby any breaches of security are immediately identified. In circumstances such as these, it will be necessary that individuals / agencies that are caught breaching or attempting to breach security are punished under internal disciplinary procedures or the Computer Misuse Act as appropriate.

Secondly, authorised users of the PND need to understand the security access level that they have been granted and the reasons behind that decision. It is strongly recommended that users are reminded of the Computer Misuse Act and that improper use of the PND could result in disciplinary procedures or prosecution. To secure the system further, all user activities on the PND will be auditable.

#### **14. Official Secrets Act 1989 (OSA)**

Individuals with authorised access to the PND will need to be made fully aware of their duties under the Official Secrets Act 1989.

Individuals working with sensitive information are commonly required to sign a statement to the effect that they agree to abide by the restrictions of the OSA. Whether this is the case or not, they are bound by the OSA's requirements.

For the purposes of the PND, it should be noted that the act applies in England, Wales, Scotland, Northern Ireland, the Isle of Man and the Channel Islands.

#### **15. Management of Police Information (MoPI) Code of Practice and Guidance**

The MoPI Code of Practice and Guidance form a package that Chief Officers must have 'due regard' to under the terms of the Police Act 1996. The development and ongoing functionality of the PND must take into consideration the management of police information and intelligence as required by MoPI. Particular consideration should be given to the following six business areas:

- Crime;
- Intelligence;
- Domestic Violence;
- Child Abuse Investigation;
- Firearms licensing; and
- Custody

The Code and Guidance set out a framework for the management of police information based on the principle that effective policing is dependant on efficient information management. It is essential that a policing purpose is established in order for information to be legally held. All aspects of the Code and the Guidance need to be incorporated into the work towards the development and implementation of the PND.

#### **Step 4 – Criteria for Data Protection Act compliance checks.**

*Does the project involve the handling of any data that is 'personal data' as that term is used in the Data Protection Act?*

**Yes** – the development of the PND does involve the handling of personal data as defined in the Data Protection Act.

A full Data Protection Act compliance check will therefore need to be undertaken.

In addition to being made available to the public via the NPIA website, copies of the public consultation on Equality, Diversity and Privacy were sent to the organisations listed below.

**Police Organisations:**

Association of Chief Police Officers

Association of Police Authorities

Her Majesty's Inspectorate of Constabulary

**Police Staff Associations:**

Police Federation

The Police Superintendents' Association

**Police Support Organisations:**

British Association of Women Police

Christian Police Association

Gay Police Association

National Association of Muslim Police

National Black Police Association

National Disabled Police Association

**Government Departments and Agencies:**

Criminal Cases Review Commission

Home Office (Home Office Disability Network)

Ministry of Justice

**Other interested individuals, groups or organisations:**

Age Concern

Blink

Commission for Equality and Human Rights

Crime Concern

East London Black Women's Organisation

Employers' Forum on Age  
Employers' Forum on Disability  
Employment Opportunities for People with Disabilities  
GLADD  
Help the Aged  
Information Commissioner\*  
Liberty  
Mind  
Muslim Council of Britain  
NACRO  
National Youth Agency  
Newham Asian Women's Project  
No2ID  
RADAR  
Refugee Council  
RNIB  
Skills for Justice  
Stonewall  
The Gender Trust  
The Interfaith Network for the UK  
The UK Intersex Association  
Trident Independent Advisory Group  
UK Youth  
UK Youth Parliament  
Unison  
Victim Support  
Women and Equality Unit  
Youth Justice Board

The IMPACT Programme would like to thank the following bodies and individuals who responded to the Equality, Diversity and Privacy Consultation.

Cheshire Constabulary

Cleveland Police Authority

Chairman of the Independent Advisory Group, Greater Manchester Police Authority

Cumbria Police Authority

Durham Constabulary

Gay Police Association  
Greater Manchester Police Authority  
Hertfordshire Constabulary  
Information Commissioners Office  
Lincolnshire Police Authority  
North Wales Police  
Northumbria Police  
South Yorkshire Police  
Sussex Police  
The British Association for Women in Policing  
The Welsh Language Board  
West Yorkshire Police

## **Key principles for ensuring the PND is privacy friendly**

- (i) Information must be used lawfully and fairly – having regard not just to individuals' rights, but also to their legitimate expectations.
- (ii) The purposes for which information is obtained and how it may be used for the PND should be clearly defined and communicated to stakeholders and the public.
- (iii) Information on the PND must be adequate, relevant, not excessive, accurate and up-to-date.
- (iv) Users must be aware of the general restrictions and liabilities associated with use of the PND, and use of the data must be controlled and audited.
- (v) Data retention must comply with protocols based on privacy standards and rules of proportionality consistent with legislation, MoPI and ACPO Retention Guidelines.
- (vi) Data must be kept and processed securely including, where appropriate, in accordance with the guidance on the Government Protective Marking Scheme.
- (vii) Individuals will be able to exercise their rights (as set out in the Data Protection Act and other legislation) efficiently, and those rights will be respected and dealt with consistently.
- (viii) There will be an agreed and consistent approach to the provision of, or access to, PND data to or by third parties
- (ix) There will be an agreed and consistent approach to responding to enforcement action (including that set out in Part V of the Data Protection Act).

A further principle was also considered:

- (x) How the PND operates, and how the system or data on it are used, will be non-discriminatory and as such compliant with the requirements of equal opportunities and diversity legislation.

This relates more to the Equality Impact Assessment work so is covered in the report on that rather than in this PIA.

## **PND processes**

### **Identity and Access Management**

The Identity and Access Management processes cover access to the system by authorised users. It comprises the following: (1) the setting up and management of user accounts; (2) rules governing access to the PND as a whole; and (3) rules governing access to individual data sets and functionality (e.g. role based access).

### **Load / store**

The Load / store processes comprise the following: (1) extraction of data from local systems by stakeholders, validation and transformation of extracted data, again by stakeholders, and transport by stakeholders to the PND – these are primarily the responsibility of the data providers; (2) ongoing loading, storage and validation of data on the PND; and (3) the ongoing process of creating, reviewing, updating, amending, weeding and deleting data on the PND.

### **Search**

The Search processes comprise the interrogation and retrieval of data from the PND, and the facility to read, download, save and, in some cases, extract and export the results of searches.

### **Associate**

The Associate processes will identify related or connected information within the PND, and will store data about those relationships or connections.

### **Flags / Markers**

These processes will enable flags and markers to be added to data items. Flags enable information to be received back (such as when someone accesses or changes that information), markers allow additional information to be provided.

### **Data use**

Data use comprises the rules about what users are entitled to do with data obtained from the PND, any steps which must be taken before acting on that information and prohibitions on use which may apply to specific categories of data.

### **Audit**

The Audit processes comprise the logging of user activity and the audit / monitoring of user activity.

### **Dealing with Subject Access Requests (SARs), FOI requests**

This comprises the processing of requests by data subjects, or others, for information held on the PND, and dealing with the other rights of data subjects under the Data Protection Act such as to prevent processing likely to cause substantial harm or distress and to have inaccurate information rectified, blocked, erased or destroyed.

### **Management Information**

This comprises the processes of examining and reporting on the operation of the PND.

### **List of groups Engaged in Consultation**

The following groups and individuals generously gave their time to meet with representatives of the NPIA and have helped to inform the contents of this report.

Association of Police Authorities

Cambridgeshire Police Independent Advisory Group (Members of Police Authority also attended)

Crescent Community Radio Station, Rochdale

Gypsy Traveller representatives for the North West

Hate Crime Panel - Leicestershire

Inter Faith Network for the UK

Nottingham & Derbyshire Methodist Volunteer Group

MIND

NACRO

Information Commissioners Office

Refugee Council

Stonewall

Victim Support

Voice UK

## Glossary

ACPO	Association of Chief Police Officers
APA	Association of Police Authorities
GPMS	Government Protective Marking Scheme
HMIC	Her Majesty's Inspectorate of Constabulary
IAM	Identity and Access Management
ICO	Information Commissioner's Office
INI	IMPACT Nominal Index
MoPI	Management of Police Information
NIM	National Intelligence Model
NPIA	National Policing Improvement Agency
OGC	Office of Government Commerce
PETS	Privacy-Enhancing Technologies
PIA	Privacy Impact Assessment
PITO	Police IT Organisation
PLX	Police Local Cross-Check
PNC	Police National Computer
PND	Police National Database
RBAC	Role Based Access Controls