A Balanced Approach

Independent Review by Sunita Mason

Safeguarding the public through the fair and proportionate use of accurate criminal record information
1. On the 7th September 2009, I was appointed as the Independent Advisor for Criminality Information Management. My role is to provide independent advice to Government on how it can best use criminality information to serve and protect the public while respecting the rights of the individual.

2. This role is wide ranging and touches on important issues about how Government departments and law enforcement agencies share information to protect the public. Part of my role is to consider the increasing public debate on the use of personal information held by Government agencies.

3. At the time of my appointment, the retention and use of criminal record information held by the police on the Police National Computer (PNC) was being argued in court. Given the nature of my role and the emerging debate, the Home Secretary asked me to conduct a review of PNC retention and disclosure arrangements to provide an independent perspective on whether a more proportionate approach could be taken.

4. My full terms of reference are set out in Appendix A. There are two elements to my review. The first is in relation to the policy on retention of criminal records on the PNC, which is about holding the information. The second is in relation to the policy on disclosure of criminal records on the PNC, which is about how the information can be obtained and used by third parties.

5. As the latter covers a very broad area, I have taken a pragmatic approach and focused my findings on obtaining and disclosing information for the purposes of employment vetting. This forms a significant part of the disclosure landscape and by focusing my approach I have been able to make practical recommendations.

6. In addressing the issues above, I have structured my report in the following way. Section 3 of the report deals with the current retention policy and my views on whether any criminal record information should be subject to deletion. In Section 4 I have considered the issue of whether access to PNC criminal record information should be limited for the purposes of employment vetting. Finally, I have looked at how disclosure arrangements can be made more accessible to employers and individuals.

Background to the Review

7. The debate around what criminal records should be held on the PNC, and for what length of time, started to surface more clearly in 2009 when the issues were raised in a case commonly referred to as the “Five Constables Case”.

---

Footnote:
1 Criminality information is any information relevant to the prevention, investigation, prosecution and penalising of crime (Magee Review of Criminality Information (July 2008))
8. The case arose from action taken by the Information Commissioner against five police forces in relation to information held on five individuals which, he argued, should have been deleted from the PNC because they involved relatively old and minor criminal records.

9. The information held in one of those instances related to a reprimand that was recorded when the individual was 13. In the other four cases the individuals were convicted in court of what, it could be argued, were relatively minor offences.

10. They became aware that these details were recorded on the PNC when in one case the individual requested details to support a visa application and in the other cases the information was disclosed to prospective employers as part of pre-employment checks. The main feature with all five cases referred to the fact that the information was held and subsequently disclosed to the detriment of the individual, which it was argued, was not proportionate.

11. The Information Commissioner took these cases up on behalf of the individuals as breaches of the 3rd and 5th Data Protection Principles. He argued that the data was irrelevant and excessive for the purposes for which it was being held and that it was not being used for the purposes for which it was being collected. This was contrary to the police view that criminal records are critical for core police purposes and for other areas of the criminal justice system such as providing full antecedent history to a court.

12. The case culminated with a Court of Appeal hearing in July 2009 and a judgment was handed down in October 2009. The judges were unanimous in giving a strong view that the police should determine what information is kept and agreed that deletion was not required in the cases at issue. They agreed that retention in these cases did not contravene the Data Protection Principles because it was consistent with the purposes specified by the police.

13. Although the judges recognised that criminal record information should be retained by the police on the PNC, they did recognise that there is a real and different set of issues around access to and disclosure of these records. Given the subject of the appeal the judges did not feel that it was their role to discuss or pass judgment on these issues.

14. Similarly to the judges, the Information Commissioner was also concerned with the issue of disclosure because he felt the information held was being used for purposes beyond that for which it was being collected therefore breaching data protection legislation.

---

2 A summary of the Data Protection Act 1998 and the principles is provided in Appendix B
15. Given the strong views on the issues around access to and disclosure of criminal record information held on the PNC, this was included within the factors that I would need to consider as part of my review.

Wider Debate on Proportionality

16. Technological advances in recent years have resulted in greater transparency in the way that governments operate. People are more able to interact, share and obtain information. Increasingly questions are being asked about what information Government needs to perform its core functions for public protection balanced against the rights of the individual.

17. The question of proportionality has arisen most recently in areas such as how Government is implementing the new Vetting and Barring Scheme and how DNA is being recorded, stored and used. These are ongoing debates and are being considered in a number of different forums such as through Parliament and/or by other Independent Advisors, think tanks and research groups. In order to look at the issue of proportionality in relation to the PNC, I am aware that my report is part of a wider debate and as highlighted in my terms of reference, I have considered where appropriate the issues and findings of others as part of my analysis.

18. In looking at the issue of proportionality, and the balancing exercise of assessing risk to the public, I have also focused on the need to avoid criminalisation of young people and adults who may have committed minor crimes or misdemeanours many years previously with no further offending thereafter. There is a need to avoid stigmatising those people who wish to follow a chosen occupation. While proper checks must remain in place to ensure public protection, we must also allow for individuals to recover from their past and continue to contribute to society.

19. Whilst it is undeniable that previous convictions (and some allegations) might be relevant when considering suitability to work - especially with children and vulnerable adults - it is also true that many lives have been impacted upon by the disclosure of minor, aged crimes and unfounded allegations.

20. Although there is general support for the use of criminality information to aid public protection, there is also considerable concern that such use may lead to an increasing number of blighted lives.

21. Such concerns may play an increasing part in the public’s decision on whether to enter into teaching roles, work with the young or vulnerable, help at local sports clubs, become involved in children’s activities such as scouting and so on.
22. My report looks at the key areas of retention and disclosure of data on the PNC and is just one aspect of the ongoing process to improve safeguarding of vulnerable members of our society. As part of the wider picture, the Government must continually review its duty to protect the public, balanced against the need to safeguard individual freedoms and rights.

23. Public safety is a joint venture between Government, employers and the individual. Employers cannot fully discharge their responsibility on the basis of Criminal Record Bureau (CRB) checks and Independent Safeguarding Authority (ISA) vetting, nor should parents cease to be vigilant in their duty of care to a child.

24. Finally, it must be recognised that no system, no matter how carefully thought out or developed, will ever totally eliminate risk. Therefore a sensible approach should be followed in balancing public protection and personal freedom.

My Approach

25. I have taken into account the outcome of ongoing reviews by various stakeholders, responses to court rulings both in the UK and European courts and also the concerns expressed through various outlets by the general public and other interested parties.

26. Given that my role is part-time and I commenced the review after the Court of Appeal judgment was handed down in October 2009, I recognise that I have not had the opportunity to consult with all those who may have an interest in this area of work. If any of my recommendations are taken forward then Government may wish to consult further on the practical implementation.

27. I have been ably assisted by members of various bodies and I am grateful for their support, clarity, willingness to discuss and desire to seek an outcome that best protects the people they serve. I have listed in Appendix C those who have contributed to this report through meetings, discussion or general assistance. I am especially grateful to Jamila Mensah, my private secretary, who has supported me in preparing this report.
If my recommendations are accepted then:

Retention of Criminal Records

i. There should be no requirement for deletion of criminal records from the Police National Computer, other than deletion of records at age 100.

ii. Adequate provision will be made to ensure that records are automatically deleted at the age of 100.

iii. All non-police users of the Police National Computer will be subject to external audit by a relevant body (such as Her Majesty’s Inspectorate of Constabulary), similar to the police, with the cost of such audit being borne by the relevant organisation.

iv. With suitable controls in place regarding the Police National Computer / Police National Database, together with a principled approach to access and disclosure, these will be sufficient tools to support public protection arrangements without unduly infringing public rights. The case for a national database that is different from the Police National Computer / Police National Database is not yet established.

Disclosure of Police National Computer Records for Employment Vetting

v. Information provided from the Police National Computer in relation to employment checks will be filtered, using specified business rules, so that employers are not given each and every piece of criminal record information. This would mean that certain old and minor records are never disclosed by the Criminal Records Bureau to the employer, which on balance I conclude is a more proportionate approach. However the current arrangements for the Independent Safeguarding Authority will be maintained to allow it to discharge its safeguarding functions.

vi. A number of interested parties will be brought together as an expert panel to advise Government on the filtering rules that should be applied to any new legislative arrangements.

vii. Government will assess the feasibility of my two practical suggestions to implement filtering so that it can identify the most cost effective solution.
viii. Part V of the Police Act\(^4\) will be amended to reflect the new filtering process.

ix. Section 4(4) of the Rehabilitation of Offenders Act 1974 will be examined and changed as a priority so that my previous recommendations can be fully implemented.

x. Government will review the Rehabilitation of Offenders Act 1974\(^5\) at the earliest opportunity to ensure it remains an effective part of the disclosure process.

xi. Government will give further consideration to the issue of soft intelligence disclosure because I believe a more balanced approach can be taken on this complex issue.

xii. Government will review the dual operation of the two separate agencies operating within the employment vetting landscape. Process integration could be considered at some stage in the future, after the ISA has become fully established. This could offer cost-savings and reductions in bureaucracy.

Guidance

xiii. Guidance for employers on how to interpret disclosure material will be developed and made more accessible. If my recommendation on filtering old and minor criminal records is adopted then it seems sensible to develop and launch any guidance simultaneously.

xiv. Clear guidance for individuals, to foster greater public understanding, will be issued.

---

\(^4\) Part V of the Police Act 1997 (c. 50) available at [http://www.statutelaw.gov.uk/legResults.aspx?LegType=All+Legislation&title=police+act+&Year=1997&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&TYPE=QS&NavFrom=0&activeTextDocId=1976347&pageNumber=1&sortAlpha=0](http://www.statutelaw.gov.uk/legResults.aspx?LegType=All+Legislation&title=police+act+&Year=1997&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&TYPE=QS&NavFrom=0&activeTextDocId=1976347&pageNumber=1&sortAlpha=0)

\(^5\) Rehabilitation of Offenders Act 1974 (c. 53) available at [http://www.statutelaw.gov.uk/legResults.aspx?LegType=All+Legislation&title=rehabilitation+of+offenders+act+&Year=1974&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&TYPE=QS&NavFrom=0&activeTextDocId=1776430&pageNumber=1&sortAlpha=0](http://www.statutelaw.gov.uk/legResults.aspx?LegType=All+Legislation&title=rehabilitation+of+offenders+act+&Year=1974&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&TYPE=QS&NavFrom=0&activeTextDocId=1776430&pageNumber=1&sortAlpha=0)
28. When reviewing the retention and disclosure policy, it is useful to consider a brief overview of the associated agencies who are chiefly responsible for collecting, storing and disclosing criminal record information. In this section, I will focus primarily on the process for holding information on the PNC and in Section 4 I will focus more specifically on the agencies involved in obtaining and using this information.

The Police National Computer

29. The PNC is a computer system for England and Wales governed by section 27(4) of the Police and Criminal Evidence Act 1984. It is used to record convictions, cautions, reprimands and warnings for any offence punishable by imprisonment and any other offence that is specified within regulations. The PNC is maintained by the National Policing Improvement Agency (NPIA) and is used by all police forces in England and Wales carrying out their policing duties.

30. The PNC went live in 1974, initially storing details of stolen vehicles. Its use and function has evolved over time and in recent years the range of facilities, level of detail and potential value of information stored on the PNC has grown considerably and gives access 24 hours a day to information of both national and local significance. The system can link into a number of separate databases and can access a range of records such as:

- Information on persons who have been convicted, cautioned or recently arrested.
- Details of registered keeper of each motor vehicle.
- Details of people who have driving licences or are disqualified from holding one.
- Details of certain types of stolen and recovered property including, animals, firearms, trailers, plant machinery and engines.
- Details of people on the National Firearms Certificate Holders register.

31. As of February 2010 there were over 9.7 million nominal records held on the PNC.

Access to the Police National Computer

32. The PNC is used by other agencies/departments, both within the criminal justice system and beyond, for core public protection purposes. Information provided fulfils functions such as supplying a court with the full history of an individual’s previous conviction history, vetting prospective employees, providing certificates for those seeking a visa for other countries, and checking those seeking visas to enter the UK.

---

6 The National Police Records (Recordable Offences) Regulations 2000 (SI 2000/1139) s
7 PNC Services, NPIA
33. There are a number of organisations with full access to the PNC, including all territorial police forces of Great Britain, HM Inspectorate of Constabulary and the Serious Organised Crime Agency (SOCA). In addition, a number of other organisations have restricted access such as HM Court Service, the Probation Service and the Departments for Transport and Works & Pension.

34. The police recognise that other organisations have a legitimate need for access to information held on the PNC and have established governance arrangements to manage and review access to it. All organisations must have a strong business case and prove they have appropriate security arrangements in place to manage the information before access is granted. In all cases where access is provided it is limited to specific roles that require it.

Current Retention Policy and the Way Forward

35. Criminal record information on an individual that is held on the PNC is stored for 100 years from their date of birth. The Court of Appeal has endorsed this retention period.

36. The Court of Appeal recognised the value of this information to the police in conducting their statutory and common law responsibilities. In particular, that this information is an important part of police investigations and can be vital in certain circumstances. For example, information held on the PNC can be useful in detecting and solving historic cases, such as rape, where there is no forensic evidence available.

37. I recognise the importance of retaining information on the PNC. For the purposes of public protection there needs to be strong evidence available to assess and form a comprehensive view of what information is essential to retain and what is not. To make any recommendations regarding the deletion of PNC data I would have to be assured that any deletion did not affect public protection.

38. In looking at this issue and gathering evidence, I have considered criminal record retention in other European jurisdictions to assess whether there is a consistent approach or policy that is commonly used or adopted. My findings are attached at Appendix D.

39. I have noticed that in some countries, all criminal records are retained until the offender reaches a particular age. In others, criminal records are expunged automatically after a set period of time or may be expunged after a period of time depending on the length of the original sentence imposed.
40. Where they are expunged, the rules governing what and when vary significantly. The differences between countries occur for a number of reasons, such as legislation, types of offences, governance, IT infrastructure etc. However, one of the noticeable elements of those that do delete full criminal records is the age at which they choose to do this. The age appears to range between 80-100 years of a person’s date of birth. This highlights that they are retaining the information for a considerable period of time, in a similar manner to the approach taken in England and Wales.

41. In Scotland there are plans to review the age of deletion (currently 70 yrs) in recognition that the average age of the population is increasing. For example, volunteers working with children could be from that age-range which means that previous information held on them could be of value for safeguarding. I understand that the Netherlands are also looking at their arrangements for similar reasons.

42. Looking at the different approaches adopted by the 26 countries I reviewed there is little consistency between them in terms of the duration that information is held. Therefore, there is no specific retention period in this context that can be identified and recommended for England and Wales.

43. There is also limited research and analysis that can be drawn upon which looks at the impact of differing retention periods on public protection arrangements. In looking to the future, in particular with the current debate on DNA retention, Government may wish to commission research in this area.

44. The Court of Appeal judgment on 15 October 2009 was based on consideration of information, evidence and statements from a range of sources in relation to PNC retention and safeguarding. Without any further clear evidence to the contrary I have concluded, on balance, that it is sensible to take the lead from the steer delivered by the Court of Appeal.

I recommend there should be no requirement at this stage for deletion of criminal records from the Police National Computer, other than deletion of records at the age of 100 (recommendation 1).

45. Although the software to implement deletion at age 100 has been developed, at present the deletion does not yet occur. I have been informed that some 4,000 records will be immediately affected. There have been no suggestions made to me that deletion at this age would pose a risk to public protection.

I recommend that adequate provision be made to ensure records are automatically deleted at the age of 100 (recommendation 2).
46. I am aware that the Information Commissioner is seeking to challenge the Court of Appeal decision on data retention in the Supreme Court. Even if this is successful it may take a considerable period of time for a decision to be taken due to the lengthy court processes involved. It is likely that the Government would then be required to issue a consultation and review of the position, such as they did in the case of S & Marper⁸ in relation to DNA retention. However, I believe there is a need for a clear policy direction now rather than in response to potential future judgments.

**Strengthening Retention Arrangements**

47. In recommending that the retention arrangements remain the same it is crucial that, as the level of stored information increases and more and more organisations request access to those data sources, sufficient controls are in place to regulate access and disclosure.

48. Recent media attention has highlighted public concern over security of information and loss of data by Government organisations.

49. In an information age it is vital that the public have confidence in the sanctity and security of that information.

50. The security of the PNC from both a physical and user point of view, is crucial given that the amount of data stored on it is likely to increase both in quantity and scope. In reviewing arrangements I spoke to HM Inspectorate of Constabulary (HMIC), the Association of Chief Police Officers (ACPO), the Metropolitan Police and was personally shown the codes of practice and guidelines⁹, levels of security on the PNC, audit trails and evidence of regular inspection by HMIC of the use of the PNC within the police force. Therefore I am assured that the police have appropriate safeguards in place.

51. As mentioned earlier in my report, the police only grant access to other users after considerable care and due consideration. Although such controls may seem onerous it is only right and proper that these are maintained at a high level and they maintain tight control over which organisations have access to the PNC.

52. In looking at these other organisations who have access to the PNC I became aware that they have different standards of auditing. At present, external organisations that have access to the PNC are required to self-audit to ensure proper compliance.

---


⁹ A statutory code of practice and guidelines known as the Management of Police Information framework (MOPi) are currently being rolled out across all police forces to ensure information is accessible and is managed in a consistent way.
I recommend that all non-police users of the Police National Computer to be subject to external audit by a relevant body (such as Her Majesty’s Inspectorate of Constabularies), similarly to the police, with the cost of such audit being born by the relevant organisation (recommendation 3).

53. An external auditing process would ensure that a consistent standard of compliance exists across all users of the PNC. To date I have seen no actual evidence that the self auditing process is not secure but it is more likely that usage is robustly challenged when someone external to an organisation questions arrangements and compliance.

Changing Landscape

54. I recognise that there are a number of changes that are occurring within the police service to better manage and share the information that is held. As the different programmes of work develop this is likely to have an interface with, and impact on, how the PNC is used.

55. One of the significant developments that is taking place is the development of a Police National Database (PND) which will provide a national system for all police forces within England and Wales to share, access and search local intelligence. The development of the database is in response to a recommendation from the Bichard Inquiry10 into the Soham murders.

56. As the database develops there will be discussions and frameworks set to govern the storage and use of the intelligence within the police service. Similarly, access that is legitimately required by other agencies for the purposes of public protection will also be agreed.

57. With the emergence of an additional national system that may feature prominently on the public protection landscape, I am aware that there have been calls by the Information Commissioner’s Office to consider an alternative to the PNC/PND whereby information is held nationally by an independent agency that would act on behalf of all public protection bodies.

58. Although my terms of reference are relatively narrow and are aimed at dealing with how information is managed on the PNC, in looking at the issues I did need to consider whether the PNC is an appropriate tool to manage criminal record information.

59. Through the various consultations I held during my review, there were references by other consultees about the need for a national public protection database, as opposed to the PNC. These calls appear to be related to the increasing volume of information being retained by the police, aligned with the growing demands by other public protection agencies to use this information.

60. In order to bring something completely new into existence there would be significant cost to the taxpayer. Furthermore the timescales would be lengthy which would mean that any changes would not take place for years. I do not consider this to be a practical approach as the stance I wish to take envisages some immediate changes that can be made to improve the system.

I believe that with suitable controls in place regarding the Police National Computer / Police National Database, together with a principled approach to access and disclosure, these are sufficient tools to support public protection arrangements without unduly infringing public rights. Therefore I recommend that the case for a national database that is different from the Police National Computer / Police National Database is not yet established (recommendation 4).
61. The disclosure of information from the PNC is a vitally important issue as it has the potential to impact severely on an individual. Drawing upon the Five Constables case, I believe the key issue was not necessarily whether the information was actually being retained but, rather, the consequences that flowed from its disclosure.

Employment Vetting – the Current Disclosure Process

62. It is normal practice for employers to carry out background checks on individuals before giving them a job. The level of checking will normally vary depending upon the type of position being offered and the potential risks attached to that role.

63. This may include references from previous employers, credit status, immigration status, qualifications attained and, possibly, checking a prospective employee’s criminal history - especially where the employee may be in a position of trust or working with vulnerable adults or children.

64. The CRB was set up in March 2002 to provide a service to employers / third parties to enable them to access the criminal record information they are entitled to - dependent upon the employment position they are filling. An individual will normally consent to this process when completing and signing an application form.

65. In simple terms, the CRB accesses criminal records from the PNC and provides a copy to the employer for their consideration. This process, known as the disclosure process, is governed by Part V of the Police Act 1997.

The Rehabilitation of Offenders Act

66. The Rehabilitation of Offenders Act 1974 (ROA) provides a protection for those that have been convicted of a criminal offence (or given a conditional caution) and who have become ‘rehabilitated’.

67. In summary, anyone who receives a sentence of not more than two and a half years imprisonment and is not reconvicted of a further offence during a time known as the ‘rehabilitation period’, is considered rehabilitated and their conviction becomes ‘spent’. This means that in some circumstances that person does not have to reveal or admit its existence. The length of the rehabilitation period depends on the sentence given for the original offence and runs from the date of the conviction.

11 Will be referred to as employers throughout the remainders of the report
68. However, there are many exceptions to ‘spent’ convictions being disclosed and these are listed in the Exceptions Order to the ROA. The two main exceptions relate to working with children or working with vulnerable adults. In these situations both spent and unspent criminal records from the PNC will be disclosed, so long as the applicant confirms that they can be asked about both types of conviction.

69. To manage the different types of criminal record information that can legitimately be disclosed to employers, the CRB operates two types of disclosures. A standard disclosure is required for those in certain professions such as members of the legal and accountancy professions, specified financial services functions and certain licensing functions such as those of the Security Industry Authority. This type of disclosure contains details of all conviction information held in England and Wales on the PNC, as well as details of any cautions, reprimands and warnings. This means that in the case of convictions, both spent and unspent are disclosed.

70. An enhanced disclosure is relevant primarily for those working with children or vulnerable adults. Examples include a teacher, scout or guide leader. Enhanced checks are also issued for certain statutory purposes such as gaming licences and judicial appointments. It contains the same information as a standard disclosure with the addition of any locally held police information relevant to the job applied for which the police consider ought to be disclosed. Where requested it will also show where an individual is included on one of the barring lists or that the individual is subject to monitoring by the ISA.

71. As well as the two types of disclosure outlined above, a person can apply for what is known as a basic disclosure as a means of providing evidence of their criminal record. This will only contain details of current convictions (ie not spent) and the service for this is operated by Disclosure Scotland, as opposed to the CRB.

Recent Changes to Employment Vetting

72. There have been recent changes made to employment checks following the introduction of the Safeguarding Vulnerable Groups Act 2006. I will briefly explain some of these changes because they have a strong bearing on my later recommendations regarding access to the PNC.

---

12 The ROA covers spent conviction and spent cautions, conditional cautions, warnings and reprimands. For the purposes of this report where I refer to ‘spent convictions’ this will incorporate all the types indicated in my previous sentence
13 Rehabilitation of Offenders Act Exceptions Order 1975 (SI 1975/1023)
14 The process is illustrated in diagram 1, Appendix F
15 The process is illustrated in diagram 2, Appendix F
16 The new barred Lists and will replace the Protection of Children Act (PoCA) List, the Protection of Vulnerable Adults (PoVA) List in England and Wales, and List 99
73. The Safeguarding Vulnerable Groups Act 2006 established the new Vetting and Barring Scheme in England, Wales and Northern Ireland. The scheme introduced enhanced vetting arrangements for those wishing to work with vulnerable groups (specifically children and vulnerable adults) and is delivered in partnership by the CRB and the ISA. The Scottish Government operates a similar and aligned scheme.

74. Under the Scheme, it is a legal requirement for those wishing to work with vulnerable groups to be registered with the ISA. The ISA will maintain two barred lists in relation to children and vulnerable adults and be responsible for that decision making process. This will prevent the most unsuitable individuals from working with vulnerable groups.

75. The primary task of the ISA will be to assess the risk of harm that an individual would pose if they were to work with vulnerable groups, based on any information held about that individual. The ISA will collate information from a range of sources including, but not limited to, data on the PNC and information held locally by the police, local authorities and other similar organisations.

76. The ISA will use trained caseworkers who will decide, on a case-by-case basis, whether a person poses an on-going or potential risk and if necessary, bar an individual from working with vulnerable groups.

77. A person who is going to be on the barred list will have the right to make representations prior to the actual barring being confirmed. They can also choose to appeal to the Care Standards Tribunal if placed on the barred list but this can be done only on a point of law or maladministration.

78. The CRB will continue to support employers by providing information on a person’s full criminal record so the employer can assess them for a particular post or position. Therefore the CRB may disclose details of offences that might not lead to a bar by the ISA, but which could be relevant to an employer (for example seeking a job as a school bus driver when having a conviction for drink-driving. This information may not lead to a bar but may still be relevant when applying for a particular role).

79. Unlike the checks provided by the CRB (which are only up-to-date on the date on which they are issued), Vetting and Barring Scheme registration is subject to ongoing monitoring. Accordingly, Scheme registration is portable, for example, to a new employer or voluntary organisation.

17 See footnote 8
18 referred to as Scheme registration
Looking to the Future - Striking a Proportionate Balance

80. Disclosure is an integral part of my report and strikes at the heart of the issue when looking at the circumstances within the Five Constables case where minor and old criminal records were disclosed to employers and in one case to support a visa application.

81. Therefore starting from the point of all criminal record data being retained on the PNC, the key question I have looked at is whether it is right and/or necessary that an employer has access to all criminal record information from the PNC (and other intelligence) to assess suitability for employment.

82. Whilst I think there is a clear need for employers to have access to information to ensure that they are recruiting someone who is appropriate and suitable - especially in circumstances where an individual is working with vulnerable groups - there is also a need to balance the type of information needed to make that judgment. Most people would agree that where someone has committed a minor offence a long time ago, they do not deserve to be blighted for life.

83. It is this principle, ie the need for balance, which led to the creation of the ROA. As a society we have endorsed and recognised that people can be rehabilitated and therefore should be able to operate and function in society and the employment market on the same terms as anyone else. The ROA supports this principle but the Exceptions Order has expanded significantly over the years. Accordingly, employers are now entitled to view ‘spent’ convictions in an increasing number of cases.

84. I query whether the current list in the Exceptions Order reflects the true spirit and purpose of the original legislation which was to make a balanced risk assessment between the rights of the individual and protection of the public.

85. The current CRB system purely acts as a collation and disclosure bureau and will send out all criminal records from the PNC without any consideration of the nature of information. Therefore whatever records it contains will be disclosed to both the individual and the employer (or voluntary organisation) at the same time.

86. The CRB processes in excess of 4 million19 disclosure applications every year and of this amount they disclose conviction, caution, warning or reprimand information relating to approximately 300,000 individuals (7% of applications).

---

19 Current forecasts highlight 4.3 million disclosure applications will be issued for 2009/10. 2007/8 CRB Annual report highlighted 3.7 million disclosure applications issued
Of those 7%, the majority will only have information about one conviction, caution, warning or reprimand. It is worth noting that every time a CRB check is applied for the same information is produced, however old or minor.

This unsophisticated approach means that information may be disclosed that is unfair and/or embarrassing to the person. It could also have more serious repercussions for the individual; for example they may be refused a job or an opportunity to work for a voluntary organisation. The Five Constables case is a perfect illustration of this problem.

In my opinion, with the current system, it is unfair to place the onus on the employer to decipher all of the information presented to them on a CRB check. PNC extracts can be difficult to interpret and employers do not always have the resources and training to fully weigh up and understand what is being presented to them. Evidence suggests that employers do not always handle and interpret the information correctly and fairly. For example, an employer faced with a clean disclosure and one containing an extract from the PNC may err on the side of caution and employ the individual with the clean disclosure regardless of the nature of the PNC extract.

My view is that a more suitable system, considered against a proportionality criterion, could prevent some of these issues surfacing in the future.

Having looked at the intention of the disclosure process, the vital factor is that the information given to employers is relevant at the time of disclosure.

I recommend that information provided from the Police National Computer in relation to employment checks is filtered, using specific business rules so that employers are not given each and every piece of criminal record information. This would mean that certain old and minor records are never disclosed by the Criminal Records Bureau to the employer, which on balance I conclude is a more proportionate approach (recommendation 5).

Implementation

In order to implement my recommendations, I would suggest the following:

- Key policy departments such as the Home Office, Department for Children Schools and Families, Department of Health and delivery partners such as Police and CRB agree a policy of filtering old and minor criminal record information.
- Agreement is attained that identifies and implements a number of business rules that aim to specifically filter out minor and old conviction, caution, warning or reprimand information for disclosure purposes in a transparent and consistent way.
• Relevant legislation\textsuperscript{20} is amended to allow for certain conviction, caution, warning or reprimand information to be filtered and not disclosed to the employer or organisation.

• To ensure that arrangements for protecting vulnerable groups are maintained, the ISA should not be treated in the same way as the CRB and should maintain its current arrangements for obtaining information (ie does not have the recommended filter applied). This will enable the ISA to meet its legislative obligation to make barring decisions.

93. In referring back to the circumstances in the Five Constables case, my view is that had such a filtering system been in existence then a more proportionate outcome could have been achieved. For example if I take each individual's circumstance in that case it may have looked as follows:

• The applicant with a date of birth (DOB) 23/4/1960 applying for a CRB disclosure who committed an offence of aggravated assault in 1975 (aged 15) and had no conviction, caution, warning or reprimand instances since that date would still have the information disclosed to the employer as aggravated assault is a violent offence and therefore considered serious.

• The applicant with a DOB of 16/9/1960 who committed two offences of shoplifting in 1974 (aged 14) and had no conviction, caution, warning or reprimand instances since that date would not have the information disclosed as the offence is considered minor and the applicant was under 16 with no other offences.

• The applicant with a DOB of 23/4/1980 who committed an offence of theft in 2000 (aged 20) and was cautioned with no conviction, caution, warning or reprimand instances since that date would not have the information disclosed as the offence is considered minor and the applicant was cautioned more than five years ago.

• The applicant with a DOB of 23/9/1970 who committed an offence of fishing without a licence in 2000 (three convictions), 2001 (two convictions) and 2004 would not have the information disclosed as the offence is considered a minor offence.

• The applicant with a DOB of 23/9/1970 who committed an offence of theft and is subsequently re-convicted seven times between 1984 and 2008 of a similar offence of theft, as well as sundry motoring offences (10 in all) between 1990 and 2008. These records would be disclosed in view of the frequency and time period over which the offences occurred.

94. Through my consultation with stakeholders and looking at the history of the retention and disclosure policy for the PNC, I know that it is both feasible and practicable for a filtering system to be applied and adopted in relation to CRB disclosures. Indeed, the

\textsuperscript{20} Part V of the Police Act 1997 and the Rehabilitation of Offenders Act 1974
police had previously instigated a process which sought to restrict access to specific PNC data, which was known as 'step down'. Details of this process are contained in Appendix E.

Filtering System and Setting the Business Rules

95. As there used to be a system applied between the PNC and CRB reducing access to certain types of information, I know it is possible to instigate a new process which seeks to apply some defined rules. However I do not think it is right for any one person to identify these rules.

I recommend that a number of interested parties are brought together as an expert panel to advise Government on the filtering rules that should be applied to any new legislative arrangements (recommendation 6).

96. The panel should be set up for the sole purpose of defining and agreeing the business rules that would filter certain types of old and minor conviction information to the employer. I do not envisage the panel having an ongoing purpose. This is a discrete exercise which could be performed in a relatively swift manner.

97. Even though the panel would be setting the criteria, I think it is useful to give some examples of criteria that could be used for a filtering process for illustration. For example:

Rule 1 A spent Conviction type which **MUST ALWAYS** be disclosed to the individual and the employer even where an application is made. For example categories involving sexual offences, violent offences or drug offences.

Rule 2 A spent Conviction type that is **NEVER** disclosed to the individual or the employer irrespective of any other consideration (ie number of convictions). For example decriminalised offences.

Rule 3 Some spent conviction types that **MIGHT OR MIGHT NOT** be disclosed depending on a set of factors such as age when one committed the offence; if it was a single offence; how long ago it was; whether there have been any further offences since; what the penalty was if any at the time, and impact on the victim.

21 Or voluntary organisation, registered body.
98. I believe that it should be technically feasible to implement a proposal along the lines of the three rules. I envisage that these are not rules where subjective discretion is routinely applied and, in particular, any factors agreed under rule three should be specifically defined so that it can be applied to an Information Technology process as far as possible.

99. I would envisage that the filtering rules are reviewed once the process has been operational for a period of time so that Government can check that the line has been drawn in the most suitable place; however I think the nature and timing of such a review would be for Government to decide.

100. It should be noted that the overall safeguarding risk would still be covered by the ISA and that the filtering rules would only apply for disclosure to employers through the CRB. This ensures the employer has information that is relevant for assessing suitability.

**Practical and Legal Changes**

101. If the Government accepts my recommendation about filtering old and minor convictions, as well as setting the business rules, it will be required to consider on a practical level how this will work and the changes to relevant parts of the legislation that will need to be made to ensure this is effectively embedded.

102. I would suggest that once the business rules have been agreed, the practical application of this process is undertaken as part of the disclosure process at one of two junctures:

- At the NPIA, when the PNC disclosure extract is produced for the CRB. The filtering rules could be applied to the PNC prior to the extract being provided to the CRB.
- At the CRB. A full PNC extract is provided to the CRB whose staff then apply the filtering rules and do not disclose those cases that have been matched to the employer.

I recommend that the Government assess the feasibility of my two practical suggestions to implement filtering so it can identify the most cost-effective solution (recommendation 7).

103. My enquiries with the NPIA have indicated that the relevant changes to implement rules one to three on the PNC would cost approximately £300,000 subject to various caveats and take an estimated six months from start to completion.
104. As well as technical changes, the disclosure process is governed by two core pieces of legislation, Part V of the Police Act 1997 and the ROA. Therefore to implement my recommendation the Government would need to change these pieces of legislation.

105. Part V of the Police Act 1997 would require change as it governs what information the police send to the CRB and the information that the CRB must disclose in response to an application. The change can be achieved by either amending it in its entirety by primary legislation or looking at what necessary changes could be made by secondary legislation.

I therefore recommend that Part V of the Police Act is amended (recommendation 8).

106. The ROA requires change as section 4(4) allows employers to ask an employee about spent convictions under the Exceptions Order. This means that even if the CRB did not disclose old or minor offences, a person could still be obliged to do so if asked. Therefore without changing section 4(4) there would be a loophole in the filtering process.

I recommend that section 4(4) of the Rehabilitation of Offenders Act 1974 is examined and changed as a priority so that my previous recommendations can be fully implemented (recommendation 9).

107. Throughout my consultations with both the Government and third sector agencies, reform of the ROA has been persistently raised and it has been argued that this is an outdated piece of legislation that is no longer fit for purpose. In my examination of the ROA it is clear that, as it was drafted in 1974 before the existence of the CRB and now the ISA, it could not have envisaged the current difficulties that individuals face when having to disclose spent convictions. The Government is aware of the challenges posed by the ROA as an official review was chaired by the Home Office in 2002 and a recent Private Members Bill was introduced in the House of Lords in December 2009, which is seeking to take forward the principles from the 2002 review.

I recommend that reform of the Rehabilitation of Offenders Act 1974 is necessary and the Government should review this piece of legislation at the earliest opportunity to ensure it remains an effective part of the disclosure process (recommendation 10).

Consistency Throughout

108. As highlighted throughout the report, my core focus when looking at access to PNC data has been to consider what relevant information is needed by an employer when looking at the suitability of an applicant for a post.
If the Government accepts my earlier recommendations regarding criminal record information, I have identified a further area within the disclosure process that requires additional consideration. This relates to information known as soft intelligence.

Given the timescale and scope of my review I have not considered this issue in full. However I have found it necessary to provide some views on where I believe issues of proportionality need to be looked at.

**Soft Intelligence**

Soft intelligence is information normally held by the police locally which is not a criminal record (for example allegations of sexual impropriety with someone under the age of consent). For the purpose of my report it may be helpful if I try to explain in practical terms how it is used before I move on to explain why I believe some changes need to be made for employment vetting.

In relation to the disclosure of soft intelligence for employment vetting it may only be disclosed in enhanced checks via the CRB. It can also be passed to the ISA who may use this for consideration in relation to barring decisions. In these situations, it is disclosed by the police upon a request for a CRB check only if the Chief Constable of the police force considers it relevant to the role for which the individual is applying. A standardised framework is used within the police force to determine whether the information ought to be disclosed.

For example, a teacher accused of inappropriate behaviour but not charged or subject to any further action by the police might have this information revealed to a prospective employer. The information would have been recorded locally by the police at the time of the investigation and although updated with the outcome, the information would be held and not deleted.

Therefore, soft intelligence could be disclosed whenever the individual applies for a role that requires an enhanced CRB check and it is deemed relevant. The applicant would not have the opportunity to prevent its transmission to the employer or explain the circumstances because they will only be aware it has been disclosed at the same time as the employer or voluntary organisation receives it.

By then the damage to the individual may have already been done in that they may not have got the job or voluntary role they applied for.

As with criminal record information, the Government needs to ensure that the disclosure of soft intelligence is dealt with in a balanced and consistent manner ie by balancing the rights of the individual with the need to protect the public.
117. The disclosure of soft intelligence and the impact it may have on an individual has recently been considered by the Supreme Court in the case of L-v- Commissioner for the Metropolis\textsuperscript{22}. In this case, the Supreme Court stated that Chief Constables must give due weight whether the information “ought to be disclosed” to ensure that the rights of the individual are appropriately considered.

118. In response to this case, work has been undertaken by a Disclosure Group (attended by stakeholders including the CRB and ISA) to improve the standardised decision-making process for disclosure of soft intelligence. This has led to a revised Quality Assurance Framework (QAF)\textsuperscript{23}, which is being used by the police.

119. I believe that this consistent approach to disclosure through the QAF will make a significant contribution towards a more proportionate and clear system for disclosure.

120. Even with these changes, the issue of soft intelligence is still challenging. Any use of unproven, untried “evidence” against someone, from an employment perspective, could seem to be a direct contravention of the fundamental principle that one is innocent until proven guilty.

121. It is my opinion that it is correct for the police to be able to use soft intelligence for their core policing purposes. It can be extremely important when dealing with issues of public protection. One of the issues surrounding Ian Huntley’s employment before the Soham murders was non-sharing of soft intelligence and I am conscious that we should do everything possible to prevent something like this happening again.

122. I believe it is right and proper that concerns such as those of violent or inappropriate sexual behaviour be taken into consideration when determining employment with children and vulnerable adults. However, its use outside this arena must be carefully reviewed. For example, allegations of theft might affect employment opportunities at a financial institution. However they remain simply that – allegations.

123. This poses the question of whether soft intelligence should be disclosed where it does not relate to potential employment with vulnerable adults or children.

- I recommend Government further consider the issue of soft intelligence disclosure because I believe a more balanced approach can be taken on this complex issue (recommendation 11).

124. When considering this, Government could look at the following suggested approach:


\textsuperscript{23} A process overview and explanatory guidance is included in Appendix G
• Soft intelligence is never disclosed to an employer via the CRB disclosure process\textsuperscript{24}.

• This would effectively remove the distinction between standard and enhanced CRB disclosures and put an end to the practice of unsubstantiated soft intelligence being declared to potential employers.

• Soft intelligence is still passed to the ISA for decision making on roles involving access to vulnerable children or adults. Through this process the individual would have the benefit of being able to make representations in their own defence.

125. I have not had the opportunity to examine this approach in full. However, in the course of preparing this report, it is apparent to me that changes need to be made to draw the line in the right place.

Process Integration

126. During the course of my review, I have had to carefully examine the disclosure landscape because this has an impact on arrangements regarding access to PNC data. The landscape has recently undergone some significant changes and there are now two bodies, the CRB and ISA, in England and Wales that deliver safeguarding arrangements.

127. The ISA will have an ongoing monitoring arrangement. Therefore, if it becomes aware of new relevant and information about an ISA-registered individual, it will consider whether the person should be barred and lose their ISA-registration. In this process, the CRB will act as a conduit for information to the ISA.

128. Knowing that this process is still taking shape, I would question whether and how these functions could be more efficiently carried out.

129. Disclosure Scotland operates as one process and is the Scottish equivalent of the CRB. It will incorporate barring functions when the Scottish equivalent of the SVG Act becomes law. This may provide a suitable model for consideration.

With two separate agencies employed on similar duties I recommend the Government review their dual operation. Process integration could be considered at some stage in the future, after the ISA has become fully established. This could offer cost-savings and reductions in bureaucracy (recommendation 12).

\textsuperscript{24} This new approach is illustrated in diagram 3, Appendix F
130. I believe the actual retention of information on the PNC carries less risk compared to the potential damage that could be caused by disproportionate or ill-considered disclosure. Therefore, I think it is important that all those involved in the disclosure process understand their role and take responsibility for the risks they own.

131. In looking at the element of disclosure, my report has largely focused on the Government's role in establishing a more proportionate policy and I have also examined how the key agencies work together and interface with the individual.

132. I recognise that employers and individuals carry a substantial responsibility within the disclosure process. An employer needs to interpret and assess any information they receive via a disclosure in a fair and transparent way. An individual needs to understand what they are legitimately required to disclose and have confidence in the process.

133. Employment vetting is undergoing substantial changes and various consultees have raised concerns about the lack of clear information available on how the various systems and processes now work. They have highlighted that without this knowledge the rights and responsibilities of the employers, individuals and organisations are unclear. This should be addressed.

134. Insofar as an individual is concerned, they should also have clearly signposted and accessible information in respect of holding information, obtaining information and disclosing information.
135. With various bodies holding and potentially disclosing information to interested parties, there is a need for consistency across the board.

136. The PNC, CRB and ISA amongst others are providers and distributors of both hard and soft intelligence. It is vital that information is disclosed in a manner that is consistent, standardised and compliant across all providers.

137. A balance must be struck between the rights and privacy of an individual (and their right to leave their past behind them) and the safety of the public – especially those most vulnerable.

138. In my many meetings with interested parties in the areas of retention, disclosure and safeguarding I have become aware of the strong commitment and desire for a comprehensive, proportionate and fair system. This is to be commended.

139. As part of my report I have made a number of recommendations to develop and strengthen the public protection network. I believe that the implementation of my recommendations will provide the impetus to challenge the existing framework, review areas of concern and provide clarity to the organisations who safeguard the public.

140. We may never reach the perfect balance between public safety and individual freedom, but we must always strive to do so.
Appendix A: Terms of Reference

Terms of Reference for independent review of policy on retaining and disclosing records held on the Police National Computer

1. These Terms of Reference have been agreed between the Home Secretary and the Independent Advisor for Criminality Information Management and do not impact on the independent nature of the review. They are intended to assist both parties by clarifying the scope and focus of the Advisor’s work in this area.

2. The Advisor is asked to review the policy for retaining records on the Police National Computer (PNC) and if she is of the view that revisions to that policy are required, recommend proposals that will deliver a clear, principled approach that is fair and proportionate and balances the needs of the individual and protecting the public.

3. The Advisor is asked to review the policy for the disclosure of records held on the PNC and if she is of the view that revisions to that policy are required, recommend proposals that will deliver a clear, principled approach that is fair and proportionate and balances the needs of the individual and protecting the public.

4. For these purposes, “records” are defined as records of convictions and of any other penalties (such as cautions, warnings, reprimands and penalty notices for disorder) which are or may be recorded on the PNC.

5. The Advisor should provide views on:

   (i) whether records should be subject to deletion and what criteria should be applied to that process;

   (ii) whether there should be arrangements for limiting access to records and what criteria should be applied to that process;

   (iii) what information regarding deletion/limitation of access should be provided to the subjects of records by the police and at what stages;

   (iv) how any suggested arrangements might be applied and monitored including, where possible, an indication of any additional cost.

6. Amongst the issues the Advisor should bear in mind are:

   (i) the outcome of the “5 Constables Case” which refers to the retention of criminal records on the PNC;

   (ii) the Association of Chief Police Officers’ Retention Guidelines for Nominal Records on the Police National Computer, together with the thinking and evidence underpinning those Guidelines;
(iii) the broader arrangements for police information handling set out under the Management of Police Information (MOPI) framework;

(iv) the relationship between retention arrangements and national systems supporting employment vetting, especially the CRB process (including the provisions contained in Part V of the Police Act 1997) and the Vetting and Barring Scheme which is being introduced;

(v) the arrangements for the retention of such records in other jurisdictions within the UK and in those overseas countries she thinks it helpful to consider;

(vi) the arrangements for retaining DNA and other biometric data such as fingerprints, together with the research and evidence base supporting the current development of new proposals in this area;

(vii) the need to strike a proportionate balance between public protection and personal privacy;

(viii) the impact of retention arrangements on the roles and responsibilities of other criminal justice agencies such as the courts and the Crown Prosecution Service.

7. In carrying out the review, the Advisor should consult the Association of Chief Police Officers, the Information Commissioner and such other persons and bodies as she sees fit.

The Advisor should provide the Home Secretary with a final report on the review by no later than 26 February 2010.
The Data Protection Act works in two ways – first it provides that anyone who processes personal information must comply with eight principles designed to ensure that personal information is:

1. fairly and lawfully processed
2. processed for limited purposes
3. adequate, relevant and not excessive
4. accurate and up to date
5. not kept for longer than is necessary
6. processed in line with a person's rights
7. secure
8. not transferred to countries without adequate protection.

Secondly it provides individuals with certain qualified rights, including the right to find out what personal information is held about them by businesses and organisations (subject to certain exclusions – for instance where national security might be undermined).

The Act also provides a framework to ensure that personal information is handled properly.

The Information Commissioner, appointed under the Data Protection Act, has various powers of enforcement and oversight including:

- the power to serve enforcement notices on data controllers who have contravened or are contravening any of the data protection principles
- the power to assess whether personal data is processed in compliance with the provisions of the Act

The Information Commissioner has taken up cases on behalf of individuals where they do not believe individuals are adhering to these principals.
### Appendix C: List of Contributors

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carolyn Armstrong</td>
<td>Press Office, Home Office</td>
</tr>
<tr>
<td>Kristian Armstrong</td>
<td>Central Policy Unit, UK Border Agency</td>
</tr>
<tr>
<td>Jonathan Bamford</td>
<td>Assistant Commissioner, Data Protection Development, Information</td>
</tr>
<tr>
<td></td>
<td>Commissioner’s Office</td>
</tr>
<tr>
<td>Ailsa Beaton OBE</td>
<td>Director of Information, Association of Chief Police Officers (ACPO)</td>
</tr>
<tr>
<td>Andy Bell</td>
<td>Deputy Chief Executive, Sainsbury Centre for Mental Health</td>
</tr>
<tr>
<td>Claire Bennett</td>
<td>Joint Public Protection Information Unit, Home Office</td>
</tr>
<tr>
<td>Jan Berry</td>
<td>Reducing Bureaucracy in Policing Advocate</td>
</tr>
<tr>
<td>Sir Michael Bichard</td>
<td>Executive Director, Institute for Government</td>
</tr>
<tr>
<td>Jodie Blackstock</td>
<td>Senior Legal Officer, JUSTICE</td>
</tr>
<tr>
<td>Richard Blows</td>
<td>Deputy Director, Safeguarding Operations, DCSF</td>
</tr>
<tr>
<td>David Bolt</td>
<td>Director Intelligence, Serious and Organised Crime Agency (SOCA)</td>
</tr>
<tr>
<td>Richard Bradshaw</td>
<td>Director of Offender Health, Department of Health</td>
</tr>
<tr>
<td>Tina Braithwaite</td>
<td>User Involvement Manager, Revolving Doors Agency</td>
</tr>
<tr>
<td>Keith Bristow QPM</td>
<td>Chief Constable Warwickshire Police/ Head of Crime ACPO</td>
</tr>
<tr>
<td>Tony Callaghan</td>
<td>Publishing and IT Manager, Prison Reform Trust</td>
</tr>
<tr>
<td>Kevin Cassidy</td>
<td>Police Policy Advisor, Police Division, Scottish Government</td>
</tr>
<tr>
<td>Clare Chamberlain</td>
<td>PNC Portfolio Staff Officer to ACC David Pryde, and Strategic Lead for PNC/PND, ACPO</td>
</tr>
<tr>
<td>David Cheesman</td>
<td>Joint Public Protection Information Unit, Home Office</td>
</tr>
<tr>
<td>Bruce Clark</td>
<td>Director of Policy, Cafcass</td>
</tr>
<tr>
<td>Anita Coles</td>
<td>Policy Officer, Liberty</td>
</tr>
<tr>
<td>Jon Collins</td>
<td>Campaign Director, Criminal Justice Alliance</td>
</tr>
<tr>
<td>Ivan Collister</td>
<td>Strategy Unit, Home Office</td>
</tr>
<tr>
<td>Mark Crawford</td>
<td>Vetting &amp; Safeguarding Policy Unit, Home Office</td>
</tr>
<tr>
<td>Belinda Crowe</td>
<td>Head of Information Rights Division, Ministry of Justice</td>
</tr>
<tr>
<td>Bobby Cummines FRSA</td>
<td>Chief Executive, UNLOCK</td>
</tr>
<tr>
<td>Gordon Davison</td>
<td>Head of Public Protection and Mental Health Group, NOMS</td>
</tr>
<tr>
<td>Stuart Duncan</td>
<td>Head of Delivery, Criminal Procedure Division, Scottish Govt.</td>
</tr>
<tr>
<td>Callum Dundas</td>
<td>Criminal Justice Operational Support, Scottish Police Services Authority</td>
</tr>
<tr>
<td>Niamh Eastwood</td>
<td>Head of Legal Services and Deputy Director, Release</td>
</tr>
<tr>
<td>Name</td>
<td>Occupation</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Susan Ferguson</td>
<td>Public Protection Unit, Police Division, Scottish Govt.</td>
</tr>
<tr>
<td>Ann-Marie Field</td>
<td>Joint Public Protection Information Unit, Home Office</td>
</tr>
<tr>
<td>Carlene Firmin</td>
<td>Senior Policy Officer, Race on the Agenda</td>
</tr>
<tr>
<td>Peter Gargett</td>
<td>Head of Criminal Justice, Lothian and Borders Police</td>
</tr>
<tr>
<td>Brian Gorman</td>
<td>Deputy Chief Executive, Disclosure Scotland</td>
</tr>
<tr>
<td>Christopher Graham</td>
<td>Information Commissioner</td>
</tr>
<tr>
<td>Elizabeth Hall</td>
<td>Head of Safeguarding, Cafcass</td>
</tr>
<tr>
<td>Anne Hamilton</td>
<td>Compliance Manager, Disclosure Scotland</td>
</tr>
<tr>
<td>Tyson Hepple</td>
<td>Director, Policing Policy &amp; Operations Directorate, Home Office</td>
</tr>
<tr>
<td>Oliver Hilbery</td>
<td>Project Director, Making Every Adult Matter Coalition</td>
</tr>
<tr>
<td>Michael Jackson</td>
<td>Head of Integration of Scottish Criminal Justice Information Systems, Scottish Government.</td>
</tr>
<tr>
<td>Gary Kernaghan</td>
<td>Director of Development and Operations, SOVA</td>
</tr>
<tr>
<td>Alan Lander</td>
<td>Senior Manager, Records and Liaison, Serious and Organised Crime Agency</td>
</tr>
<tr>
<td>Linda Lennon CBE</td>
<td>Chief Executive, Parole Board</td>
</tr>
<tr>
<td>Peter Lewis</td>
<td>Chief Executive, Crown Prosecution Service</td>
</tr>
<tr>
<td>Gary Linton</td>
<td>Head, ACPO Criminal Records Office (ACRO)</td>
</tr>
<tr>
<td>Steve Long</td>
<td>Chief Executive, Criminal Records Bureau</td>
</tr>
<tr>
<td>Sir Ian Magee</td>
<td>Senior Fellow, Institute for Government</td>
</tr>
<tr>
<td>Chris Mayer CBE</td>
<td>Chief Executive, HM Courts Service (HMCS)</td>
</tr>
<tr>
<td>Adrian McAllister</td>
<td>Chief Executive, Independent Safeguarding Authority</td>
</tr>
<tr>
<td>Danny McAllister</td>
<td>Director, High Security, National Offender Management Service (NOMS)</td>
</tr>
<tr>
<td>Tom McArthur</td>
<td>Director of Support to Policing Operations, NPIA</td>
</tr>
<tr>
<td>Dougal McClelland</td>
<td>Senior Business Manager, Records and Liaison, SOCA</td>
</tr>
<tr>
<td>Patricia McFarlane</td>
<td>Policing Powers and Protection Unit, Home Office</td>
</tr>
<tr>
<td>Margaret McGowan-Smyth</td>
<td>Legal Advisers Branch, Home Office</td>
</tr>
<tr>
<td>Kevin McLean</td>
<td>Director, Employment Checking Project, Home Office</td>
</tr>
<tr>
<td>Gordon McManus</td>
<td>National Intelligence Model Development Team, ACPO Scotland</td>
</tr>
<tr>
<td>Mike McMullen</td>
<td>Head of International, ACRO</td>
</tr>
<tr>
<td>Sean McNally CBE</td>
<td>Operations and Performance Director, HMCS</td>
</tr>
<tr>
<td>Name</td>
<td>Position / Organization</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>Jamila Mensah</td>
<td>Joint Public Protection Information Unit, Home Office</td>
</tr>
<tr>
<td>Clare Morgan</td>
<td>Head of Operations, Criminal Justice, SPSA</td>
</tr>
<tr>
<td>Andrew Neilson</td>
<td>Assistant Director, Howard League</td>
</tr>
<tr>
<td>Peter Neyroud QPM</td>
<td>Chief Constable &amp; Chief Executive, NPIA</td>
</tr>
<tr>
<td>John O’Brien</td>
<td>Vetting &amp; Safeguarding Policy Unit, Home Office</td>
</tr>
<tr>
<td>Sir Hugh Orde QPM, OBE</td>
<td>President, ACPO</td>
</tr>
<tr>
<td>Bill Peace</td>
<td>Deputy Director Records and Liaison, SOCA</td>
</tr>
<tr>
<td>Simon Pountain</td>
<td>Lead on Disclosure, ACPO</td>
</tr>
<tr>
<td>Ian Powell</td>
<td>Head of Member Services, British Association of Settlements and Social Action Centres (BASAC), representing Community Alliance</td>
</tr>
<tr>
<td>ACC David Pryde</td>
<td>PNC Portfolio Lead, ACPO</td>
</tr>
<tr>
<td>Jeanette Pugh</td>
<td>Director, Safeguarding Group, DCSF</td>
</tr>
<tr>
<td>Ian Readhead</td>
<td>Director of Information, ACRO</td>
</tr>
<tr>
<td>Oliver Reichardt</td>
<td>Head of Compact, National Council for Voluntary Organisations</td>
</tr>
<tr>
<td>Stephen Rimmer</td>
<td>Director General, Crime and Policing Group, Home Office</td>
</tr>
<tr>
<td>Lorraine Rogerson</td>
<td>Director Policy &amp; Administration, Attorney General’s Office</td>
</tr>
<tr>
<td>Helen Ryan</td>
<td>Head of Policy and Strategy, Criminal Records Bureau</td>
</tr>
<tr>
<td>Mr Justice Ryder</td>
<td>Presiding Judge of the Northern Circuit</td>
</tr>
<tr>
<td>Russell Scott</td>
<td>National Intelligence Model Development Team, ACPO Scotland</td>
</tr>
<tr>
<td>Sir Roger Singleton CBE</td>
<td>Chief Adviser on the Safety of Children, Chair of Independent Safeguarding Authority</td>
</tr>
<tr>
<td>David Smith</td>
<td>Deputy Commissioner, Data Protection, Information Commissioner’s Office</td>
</tr>
<tr>
<td>Michael Spurr</td>
<td>Chief Operating Officer, NOMS</td>
</tr>
<tr>
<td>Christopher Stacey</td>
<td>Information and Advice Manager, UNLOCK</td>
</tr>
<tr>
<td>LLB LLM</td>
<td></td>
</tr>
<tr>
<td>Lord Justice Thomas</td>
<td>Lord Justice of Appeal</td>
</tr>
<tr>
<td>Malcolm Thompson</td>
<td>Strategic Development Project Manager, Clinks</td>
</tr>
<tr>
<td>Peter Todd</td>
<td>Assistant Inspector of Constabulary, HMIC</td>
</tr>
<tr>
<td>Kevin Walsh</td>
<td>Joint Public Protection Information Unit, Home Office</td>
</tr>
<tr>
<td>Karl Wissgott</td>
<td>Head of PNC Services, NPIA</td>
</tr>
<tr>
<td>John Woodcock</td>
<td>Joint Public Protection Information Unit, Home Office</td>
</tr>
<tr>
<td>Jackie Worrall</td>
<td>Director of Policy and Public Affairs, Nacro</td>
</tr>
</tbody>
</table>
### Appendix D: European Approach to Criminal Records Retention

<table>
<thead>
<tr>
<th>Country</th>
<th>Governance</th>
<th>Retention policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Austria</strong></td>
<td>Maintained by the Register Division of the Federal Police Bureau (FPB) in Vienna. Nationwide and centrally managed database of criminal records containing all criminal convictions.</td>
<td>Deletion from the criminal record either 3, 5, 10 or 15 years from completion of sentence depending on the term of imprisonment and if no further convictions are added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Individuals may apply or may provide consent to a third party to the FPB who will provide a restricted certificate containing convictions that are not expunged (varies from 3-15 years depending on penalty). Some minor offences will not be included.</td>
</tr>
<tr>
<td><strong>Belgium</strong></td>
<td>Belgian Code of Criminal Procedure (Ministry of Justice)</td>
<td>Very minor sentences (e.g. community sentence &gt;45 hrs; 1-7 days imprisonment) deleted after 3 years. Otherwise no deletion.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Individuals may apply or may provide consent to a third party Two types of certificate – Model's 1 and 2 are available to Belgians working in Belgium. Model 2 carries more detail and is issued in relation to employment with children and vulnerable adults. Model 1 is the only certificate available for Belgians working abroad.</td>
</tr>
<tr>
<td><strong>Bulgaria</strong></td>
<td>Criminal Records Database regulated by the Criminal Records Bureau</td>
<td>Rehabilitation period on the criminal record depends on type of sentence; age of offender; and, in all cases, whether other offences are committed within a specific period after release from prison. Court judgments are fully removed from criminal records after a period ranging from 2-20 years depending on the term of imprisonment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Individual application or to person with power of attorney Only offences for which the applicant has not been rehabilitated (e.g. offences less than 3 years) or which have not been stepped down, are disclosed.</td>
</tr>
<tr>
<td><strong>Cyprus</strong></td>
<td>Criminal records repository is retained by the Criminal Investigations Office, Part of the Cyprus Police and affiliated to the Cyprus Ministry of Justice.</td>
<td>Convictions generally cannot be removed from an individual's criminal record, however based on the type of punishment issued by the court some offences may not be disclosed. This tends to apply to sentences served for less than 2 years.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Private citizens can apply for a Certificate of Character. The Certificate provides disclosure of criminal convictions based on the Cyprus Penal Code. Generally first-time sentences of less than three months imprisonment or a fine of less than €1,700 do not appear on the certificate.</td>
</tr>
<tr>
<td><strong>Czech Republic</strong></td>
<td>Central repository maintained by the Criminal Records Office</td>
<td>The criminal record of a convicted person is stored for 100 years from the person’s date of birth. The full record is only available for limited purposes, including court proceedings. Otherwise courts delete sentences from the criminal records after 3, 5, or 10 years depending upon the term of imprisonment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Individuals seek an Excerpt from the Penal Register, which contains information relating to convictions that have not been expunged, including information about punishable offences and sentences.</td>
</tr>
</tbody>
</table>

---

25 A detailed version different countries retention periods and rules around disclosure can be found in the following link to a KPMG study [http://www.cpni.gov.uk/ProtectingYourAssets/overseas.aspx](http://www.cpni.gov.uk/ProtectingYourAssets/overseas.aspx)
<table>
<thead>
<tr>
<th>Country</th>
<th>Governance</th>
<th>Retention policy</th>
<th>Employment Vetting Arrangements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denmark</td>
<td>The Central Criminal Records Register accessed only by the Danish police</td>
<td>Deletion 10 years after completion of sentence (including non-custodial sentence), or at age 80.</td>
<td>Individuals may apply or may provide consent to a third party. Two certificates are available domestically for use in employment with children and by police and public authorities. The certificate will contain information about any convictions, fines or discontinued charges relating to criminal offences or overseas judgments.</td>
</tr>
<tr>
<td>Estonia</td>
<td>The Punishment Register administered by the national Police Board</td>
<td>Retention of convictions is dependent upon the length of sentence. Retention periods vary from 1 to 10 years and not at all for life imprisonment. Even if the conviction is removed, the record will be stored in national archives for 50 years.</td>
<td>Individuals or third party representatives with consent. Limited or full check available both for employment purposes. The limited check provides details only of convictions from the Punishment Register (PR) relevant to employment types. Full check discloses all convictions.</td>
</tr>
<tr>
<td>Finland</td>
<td>National central register administered by the Legal Register Centre</td>
<td>Judgments will be removed from a criminal record after 5, 10 or 20 years, or at the age of 90 (or upon death) if no further convictions have been added. The length of time varies according to the seriousness of the conviction.</td>
<td>Individuals apply. This will only be issued for types of employment which involve regular contact with children. It does not constitute a full criminal record disclosure but will only contain information that is judged to be relevant to the type of employment. The existence of other types of conviction will not be indicated.</td>
</tr>
<tr>
<td>France</td>
<td>French Criminal Register</td>
<td>Records are retained until deletion on death of the person or at the age of 100. Convictions are removed from disclosure Bulletins 2 &amp; 3 between 3 and 5 years after the completion of sentence depending on the severity of the offence. For Bulletin 2, when issued for employment with children, offences against minors are also included.</td>
<td>Individuals or third party (only in cases of legal incapacity) to Ministry of Justice. Two Bulletins are available. Bulletin 2 to French administrative authorities and employers and Bulletin No 3 for use overseas.</td>
</tr>
<tr>
<td>Germany</td>
<td>Criminal records maintained by the Federal Central Criminal Register</td>
<td>Criminal conviction data is removed after certain fixed time periods (5, 10, 15 or 20 yrs) according to the type of punishment imposed. Certain types of disposals may not be deleted from the Register and this applies to lifetime imprisonment sentences and orders for psychiatric hospitalisation. All deleted convictions are retained for 1 further year but cannot be disclosed in this period.</td>
<td>Individuals or statutory representatives apply to Federal Central Criminal Register. Disclosure covers sentences by German courts, security and rehabilitation related measures, warnings or youth custodial sentences imposed.</td>
</tr>
<tr>
<td>Country</td>
<td>Governance</td>
<td>Retention policy</td>
<td>Employment Vetting Arrangements</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>-----------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Greece</td>
<td>Criminal records held by the local Public Prosecutor’s Office. Foreign national information is held by the Ministry of Justice.</td>
<td>Conviction information for adults (over 17 years of age) generally remains on the Penal Record until they the age of 81or their death. However disclosure has much shorter retention periods (3, 5, 7, 10, 20 years from end of sentence).</td>
<td>All individuals, whether or not born in Greece can apply for a copy of their Penal Record Copy (PRC). Third parties are not permitted to apply for disclosure for criminal records, with the exception of certain public positions in Greece. There are two types of PRC – a general one which applies to pre-employment screening and one for court/government (including schools), public officials and/or their offices.</td>
</tr>
<tr>
<td>Hungary</td>
<td>Central repository of criminal record information is maintained at the Criminal Records Department based at the Central Office for Administrative and Public Services.</td>
<td>The retention period depends on the type of offence, the age of the convict and also the number of convictions. Convictions have a variable expiry period of 3 to 15 years depending on the gravity of the crime committed. Criminal convictions are no longer disclosable after the end of the expiry period.</td>
<td>Applications for criminal records disclosure can be made in the form of a Certificate of Good Conduct (CGC). A CGC is issued to an individual for employment and general purposes and shows whether or not an individual has a disclosable criminal conviction registered against their name. Any convictions shown are accompanied by relevant data including details of cautions or penalties.</td>
</tr>
<tr>
<td>Ireland</td>
<td>National register of criminal records maintained by the Garda Central Vetting Unit</td>
<td>Convictions remain on record for the lifetime of the convicted individual.</td>
<td>Registered employers (security industry and where work involves unsupervised access to children or vulnerable adults) can apply for Garda Vetting Disclosure on their employees.</td>
</tr>
<tr>
<td>Italy</td>
<td>Centralised database of criminal record information is maintained at the Criminal Records Bureau.</td>
<td>Convictions remain on record until an individual reaches 80 years of age, or upon the death of an individual. Convictions may be removed in circumstances of non-custodial punishments or cancellation of convictions. Convictions of minors generally removed at 18.</td>
<td>Individual or third party with consent can apply. A penal certificate will include all convictions except for those declared by a judge to be non-disclosable</td>
</tr>
<tr>
<td>Latvia</td>
<td>National register of criminal record data, the Punishment Register.</td>
<td>Criminal convictions deleted ten years after an individual’s death. Administrative convictions deleted 10 years after sentence is completed.</td>
<td>Individuals may apply or may provide consent to a third party. Latvian employers may apply directly for disclosure where there is a regulatory requirement. Individuals, authorised third parties and employers receive a Certificate on Conviction. Individuals can ask for the live or archived register to be searched. The certificate only reveals existence of convictions – not what the convictions are.</td>
</tr>
<tr>
<td>Country</td>
<td>Governance</td>
<td>Retention policy</td>
<td>Employment Vetting Arrangements</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Lithuania</td>
<td>The Departmental Register of Suspected, Accused and Convicted Persons is a central repository of criminal record data and related information.</td>
<td>Archive data is stored for 75 years or until the convicted person has died; the criminal proceedings have been stopped, or the court has lifted the sentence. Such data is archived for 75 years. Archived data is not disclosed to other countries. For disclosure purposes, including to foreign authorities judgments are removed from the Register immediately after the completion of the sentence, or after 3, 5, 8 or 10 years, depending on the seriousness of the offence. These periods are halved for minors.</td>
<td>Individuals may apply to Ministry of Interior or provide consent to a third party. Information disclosed in the certificate is similar to that in UK disclosures.</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>Maintained in a central electronic register by the Ministry of Justice. The register holds records of convictions and sanctions from all penal courts.</td>
<td>Individual's convictions are removed once the rehabilitation period, which depends on the length of sentence, has passed. Sentences of minors are separately recorded and are not considered crimes, therefore are not transferred to the criminal register.</td>
<td>Individual receives Bulletin 3 Extrait de Casier Judiciaire (&quot;Bulletin 3&quot;) which is the only type of criminal record certificate available. This will only contain undeleted custodial sentences (i.e. no fines).</td>
</tr>
<tr>
<td>Malta</td>
<td>Central repository of criminal record information is maintained at the Criminal Records Office (CRO)</td>
<td>The CRO holds conviction details for periods dependent upon the length of a sentence. The Courts of Justice of Malta can exercise the right to prevent a conviction being registered against the name of an individual. This directive may be issued upon judgment or at any period after a hearing by the attorney general. An individual is required to apply for the removal of conviction data.</td>
<td>Residents, non-resident Maltese, including non-citizens who have resided in Malta for a significant period are eligible to apply for criminal records disclosure at the Malta Police GHQ. All live convictions will be disclosed.</td>
</tr>
<tr>
<td>Netherlands</td>
<td>The Criminal Records System is a central database of criminal records and police records data.</td>
<td>Records for serious crimes are maintained for at least 30 years (40 years for sentences over 8 years) or until the age of 80, when all records will be removed. Misdemeanour offences are registered for at least 5 years.</td>
<td>Certificates of Good Conduct may be requested for pre-employment screening. Forms require completion from both individuals and employers. Certificate only reveals information related to whether there is any behaviour which may prevent that person from undertaking a particular type of employment. It will not be a statement of all criminal history. Will cover at least 4 years and may include the full criminal history of an individual.</td>
</tr>
<tr>
<td>Country</td>
<td>Governance</td>
<td>Retention policy</td>
<td>Employment Vetting Arrangements</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>-----------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td><strong>Poland</strong></td>
<td>The National Criminal Register Information Office administers the National Criminal Register which holds a central repository of criminal records data</td>
<td>Most judgments are removed from a criminal record after 1, 3, 5 or 10 years, depending on the type of sentence passed. In the event that an individual is convicted of a sexual offence against a minor under the age of 15 years, the conviction will remain on record permanently.</td>
<td>Individuals may apply or may provide consent to a third party. Employers (though not any overseas) can apply directly without consent for disclosure in relation to some employment types (under Polish law). Convictions not removed from criminal record are disclosed.</td>
</tr>
<tr>
<td><strong>Portugal</strong></td>
<td>Central electronic register maintained by the Ministry of Justice.</td>
<td>An individual’s convictions are permanently removed from the criminal registry once the rehabilitation period has passed. Rehabilitation period depends on original sentence and can be 5, 7 or 10 years from the completion of the sentence. Criminal Record department retains convictions for a further 2 years.</td>
<td>Individuals may apply or may provide consent to a third party.</td>
</tr>
<tr>
<td><strong>Romania</strong></td>
<td>A Central Criminal Records database maintained by the General Inspectorate of the Romanian Police</td>
<td>There are specific occasions where judgments will be removed such as where the offences are decriminalised or in the event of an amnesty. A fine or sentence of up to three years is removed 20 years after completion or sentence.</td>
<td>Individuals or third parties with power of Attorney can apply directly. All convictions on database are provided.</td>
</tr>
<tr>
<td><strong>Slovakia</strong></td>
<td>A central repository of criminal record information is maintained at the Register of Crimes, which is held at the office of the General Prosecutor.</td>
<td>Record retained on live register until death, or 100 years after birth, unless conviction is overturned. After this time the information is sorted to a non-live register indefinitely.</td>
<td>Criminal Record Transcript may be issued to authorised bodies or only to individuals employed or seeking employment in the private security services or technical services industries. Authorised bodies include government ministries, the Slovak police force, the secret service or the National Bank of Slovakia.</td>
</tr>
<tr>
<td><strong>Slovenia</strong></td>
<td>The Department for Criminal Records and Educational Measures (DCREM) based at the Ministry of Justice maintains the register.</td>
<td>Various deletion periods depending on the length of imprisonment. Persons can apply for convictions to be removed so long as no further offence has been committed and half the deletion period has expired.</td>
<td>A local employer can request an employee to supply a Criminal Record Certificate (CRC), provided that disclosure of criminal records is clearly stated in the advertised vacancy. This does not apply to foreign employers. A full CRC can be obtained for certain profession such as working with children. This certificate will contain details relating to expunged convictions.</td>
</tr>
<tr>
<td>Country</td>
<td>Governance</td>
<td>Retention policy</td>
<td>Employment Vetting Arrangements</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>-----------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Spain</td>
<td>Register maintained by the Ministry of Justice</td>
<td>Deletion only possible if the convicted person has satisfied his/her civil responsibilities and that he/she has not committed another criminal offence within time periods ranging from 6 months – 5 years. This period depends on the seriousness of the offence.</td>
<td>Individuals or authorised representatives may apply to the Criminal Register of Convicted Offenders and Fugitives.</td>
</tr>
<tr>
<td>Sweden</td>
<td>Criminal Records Act (1998:620) sets out statutory framework – register maintained by Ministry of Justice</td>
<td>Fines are stored for five years. Any other sanction is stored for ten years after date of judgment, or date of release from imprisonment. Where an individual has more than one conviction reported in the criminal record, no information is deleted until the rehabilitation time has occurred for all convictions. The maximum length of time for a sentence can be held in the Swedish Criminal Record System is twenty years.</td>
<td>Applications will not be accepted from employers or other third parties under any circumstance. Five different “Registry Extracts” are available depending on the job being applied for, or whether the request is made under Freedom of Information legislation. Jobs working with children are covered by two types of Registry Extract (schools and health and rehabilitation clinics for children). Registry extracts for overseas purposes will contain all “live” convictions.</td>
</tr>
</tbody>
</table>
Appendix E: Step Down model

The Retention Guidelines for Nominal Records on the Police National Computer came into force on 31st March 2006 and were developed through negotiation and discussion.

The Guidelines were developed to restrict access to certain data fields by non-police users of the PNC, after set periods of time, whilst allowing the police continued access in support of policing purposes.

The step down model was designed to provide the police service with continuing access to data that allowed it to discharge its statutory and common law responsibilities. The records were still to be retained on PNC until the relevant person was deemed to have attained 100 years of age.

The Guidelines made reference to ‘clear periods’ in determining the time at which the offence was to be stepped down. There were rules regarding where the subject had re-offended within the ‘clear period’, then the time clock was reset from that time and a further ‘clear period’ begun.

The ‘step down’ time periods were based on the following criteria:

- The age of the subject
- The final outcome
- The sentence imposed
- The offence category

All non-conviction events, for example acquittals and arrests, would have been ‘stepped down’ when the relevant entry was made on the PNC. This would ensure that such data was only open to inspection by the police.

Following the ‘step down’ other users of PNC would be unaware of the existence of such records, save for those occasions where the individual was the subject of an Enhanced Check under the Criminal Records Bureau (CRB) vetting process.

In those cases the data would be dealt with as intelligence and only disclosed, where the relevance test had been applied, on the authority of the Chief Officer.

On 19 October 2009, following the Five Constables case, the Court of Appeal judgment came out in support of the retention of criminal convictions on the PNC. Accordingly, on 22nd October 2009, all Chief Officers were advised that the process of manually stepping down records was to cease with immediate effect and all convictions were to remain on the PNC until the individual’s 100th birthday.
Appendix F: Flow Diagrams of the Disclosure Process

Current Position – standard CRB

Employer or Organisation requests Standard CRB check

Employer or Organisation

CRB has direct access to extract from PNC Names Database

CRB
direct
CRB
requests
Standard
check

CRB dispatches clear certificate to employer

If no matches, CRB requested to print clear CRB certificate

Extract of PNC

If name matches, request sent to PNC at NERC

If name matches but unsure of correct identity, referred to senior CRB staff with live access to PNC to determine if correct identification match

All disposal history sent to CRB

PNC

Current Position – enhanced CRB

Employer or organisation requests Enhanced CRB check

Employer or Organiser

CRB has direct access to extract from PNC Names Database

CRB
direct
CRB
requests
Enhanced
check

CRB dispatches clear certificate to employer

If no matches, CRB requested to print clear CRB certificate

Extract of PNC

If name matches, request sent to PNC at NERC

If name matches but unsure of correct identity, referred to senior CRB staff with live access to PNC to determine if correct identification match

All disposal history & local intelligence sent to CRB

PNC

Individual

ISA may ask individual to make representations before making barring decision

ISA receive all data and decide whether to refer

PNC send request for local authority intelligence

Local Police Forces
Employer or organisation requests Enhanced CRB check

CRB dispatches clear certificate to employer

CRB has direct access to extract from PNC Names Database

If no matches, CRB cleared to print clear CRB certificate

If name matches (hit) request sent to PNC at Hendon

If name matches but unsure of correct identity, escalated to senior CRB staff with live access to PNC to determine if correct identification match

ISA may ask individual to make representations before making barring decision

Individual

PNC send request for local/soft intelligence

Local Police Forces

Only relevant conviction history (based on matrix) is sent to CRB

All disposal history and local intelligence sent to ISA

ISA receive all data and decide whether to bar

Employer or organisation

CRB

Proposed position

Extract of PNC

Independent Safeguarding Authority
Appendix G: Quality Assurance Framework Process and Guidance (v7.0)

MP7a - Disclosure Rationale Consideration (page 1 of 5)

Previous decision logs will have identified information about an applicant, or third party, that might be relevant. This process will consider whether the information presented is statutorily relevant and whether it ought to be considered for disclosure.

1. **START**
   - Does the application relate to either children, vulnerable adults or both?

2. **Yes**
   - Do you believe the information to be relevant to considerations of risk, having regard to the application before you?
     - You should record the rationale supporting your answer.
     - Information discarded

3. **Yes**
   - Do you believe the information to be relevant to considerations of risk, that this individual may pose to children, the vulnerable or both, having regard to the application before you?
     - You should record the rationale supporting your answer.
     - Information discarded

4. **Yes**
   - The required test:
     - "Is the information so unlikely to be true, or so lacking in substance, that it would be disproportionate to disclose?"
     - You should record the rationale supporting your answer for whether you believe the information is sufficiently credible to pass this test.
     - Information does not pass the test: Information discarded

5. **No**
   - Information passes the test

6. **Yes**
   - Consider the route by which this information is to be disclosed
     - Now go to MP7b

If you answer "Yes" to Box 1, this Method Product process may be approached in 2 distinctly different ways. You need to decide which best suits the information that you are assessing. Both options will produce the same end result however one may reduce the amount of work (audit recording) required to reach it.

You may proceed 1, 3, 4, 5 or 1, 4, 3, 5 — or use whichever sequence/method will discard the most irrelevant information at the earliest opportunity.
**MP7b - Disclosure Method Consideration (page 2 of 5)**

This process asks that you consider the most appropriate method of disclosure for the information that has A) passed all previous tests, B) is relevant and C) ought to be disclosed.

1. In your judgement will the Applicant already know all of the remaining information that you are considering for disclosure?
   - No or Unsure
   - Yes

2. Would disclosure of any of the information to the Applicant prejudice a police operation or potentially cause a crime to be committed?
   - Yes or Unsure
   - No

3. Could a ‘safe subset’ of the information be disclosed to the Applicant without prejudicing a police operation or potentially causing a crime to be committed?
   - (see Note 1)
   - Yes or Unsure

4. Could some or all of the remaining information (i.e. not the ‘safe subset’) be disclosed to the Registered Body or IBB?
   - No or Unsure
   - Yes

5. Does the risk to a police operation or the risk of a crime being committed outweigh the risk from not disclosing the remaining information?
   - No or Unsure

---

There may be rare instances where information that is relevant to the IBB may not fall within the remit of an ECRC. If this is the case, any information that should not be included on an ECRC should be redacted and sent to the IBB under separate arrangements.

**Redaction:** the separation of disclosable from non-disclosable information by blocking out individual words, sentences or paragraphs or the removal of whole pages or sections prior to release.

---

**Note 1**

'Safe subset' – a portion of relevant information that may be safely disclosed if extracted from the whole.
Note: When assessing information, if you conclude that disclosure is appropriate, but that more immediate action is required than the disclosure service can provide, consider what action may be taken to communicate your concerns in a more immediate manner. This is particularly relevant if the applicant is already in post, and a vulnerable group is in immediate danger.

Box 1
- Does the application relate to either children, vulnerable adults or both?
The Post Applied For and/or the Sector Applied For (if an ISA application) will indicate whether the application should be considered for potential risks to one or both of the vulnerable groups.
Some applications for Enhanced Disclosure will not require the applicant to have any such access — gaming and licensing applications, for example.

Box 2
- Do you believe the information to be relevant to considerations of risk, having regard to the application before you?

Box 3
- Do you believe the information to be relevant to considerations of the risk that this individual may pose to children, the vulnerable or both, having regard to the application before you?
Discard any information that, in your judgment, the prospective employer would not find material with regard to the nature of the work to be undertaken and/or the risk to a vulnerable group.
Note:
- If in doubt return a response of ‘Yes’ to allow further consideration.
- Ensure that your rationale is recorded clearly and concisely on the AT3 document, and that it includes references to the level of access/supervision and the opportunity to commit offences of a similar nature.

Box 4 (the ‘evidence test’)
- ‘Is the information so unlikely to be true, or so lacking in substance, that it would be disproportionate to disclose?’
The required test: ‘Is the information so unlikely to be true that it would be disproportionate to disclose.’
The test is passed if your answer to the test is ‘No’. If information passes the test, you continue your considerations.
Information passes the test unless there are ‘unfavorable circumstances’ that lead you “to believe that the information might not be true” or “is so devoid of substance that it would be unreasonable to conclude that it might be true” (case of X v Chief Constable of West Midlands Police’). Information need not be true beyond reasonable doubt.

Box 5 (Only used when information relates to a Third Party)
- If the information relates to a third party, do you believe there is a reasonable reason to consider that the third party may gain relevant access to children or the vulnerable through the nature of the role?
You need to satisfy yourself that the third party will have relevant access and present a risk to the vulnerable.
Discard any information relating to a third party where it is not reasonable to believe that they have/have relevant access to the vulnerable.

Box 6 (See also the related entry within the MP8)
- Do you believe that the information is both reasonable and proportionate to disclose?
Taken from the Treasury Solicitor’s Department publication ‘The Judge over your shoulder’ (recommended reading):

‘Reasonableness’ and ‘proportionality’ are separate concepts, though they sometimes produce the same result.
Reasoneableness — following a proper reasoning process and so coming to a reasonable conclusion.
Proportionate — a proportionate decision: one that went no further and was no more drastic in its effects than was necessary to secure the legitimate aim. (paraphrased)

The Courts have recognised that, when two reasonable persons are faced by the same set of facts, it is perfectly possible for them to come to different conclusions, so that a range of lawful decisions may lie within the discretion of the decision-maker. At the same time, the Courts have defined a category of decisions which lie outside that range of discretion:

- "a decision which is so outrageous in its defiance of logic or of accepted moral standards that no sensible person who had applied his mind to the question could have arrived at it";
- "beyond the range of responses open to a reasonable decision-maker".
MP7 – General Guidance 1

The nature of an Enhanced Criminal Record Certificate

Excerpt from The Police Act, Part V, Sect 115 (also incorporated in SOC and Police Act 2005)

6) An enhanced criminal record certificate is a certificate which—
(a) gives—
(i) the prescribed details of every relevant matter relating to the applicant which is recorded in central records, and
(ii) any information provided in accordance with subsection (7), or
(b) states that there is no such matter or information.

7) Before issuing an enhanced criminal record certificate the Secretary of State shall request the chief officer of every relevant police force to provide any information which, in the chief officer’s opinion—
(a) might be relevant for the purpose described in the statement under subsection (2), and
(b) ought to be included in the certificate.

8) The Secretary of State shall also request the chief officer of every relevant police force to provide any information which, in the chief officer’s opinion—
(a) might be relevant for the purpose described in the statement under subsection (2),
(b) ought not to be included in the certificate, in the interests of the prevention or detection of crime, and
(c) can, without harming those interests, be disclosed to the registered person

Case of “R(L) v The Commissioner of Police of the Metropolis, Supreme Court 2009” stated –

“The question whether the information might be relevant is not, however, the end of the matter. An opinion must also be formed as to whether it “ought” to be included in the certificate. It is here, as the guidance that is available to the police correctly recognises, that attention must be given to the impact that disclosure may have on the private lives of the applicant and of any third party who is referred to in the information. For the reasons I have already given (see paras 22-29), I consider that the decisions which the chief officer of police is required to take by section 115(7) of the 1997 Act will fall within the scope of (Article 8(1) Human Rights Act) in every case. So in every case he must consider whether there is likely to be an interference with the applicant’s private life, and if so whether that interference can be justified.”

Lord Hope

“This is to be achieved in the first place by the chief officer of police giving no less weight to the section 115(7)(b) requirement that in his opinion the information ought to be included in the certificate than to the section 115(7)(a) requirement that he thinks it might be relevant (rather than presuming that any potentially relevant information should ordinarily be disclosed).”

Lord Brown
The Wednesbury Principles
- taken from the Treasury Solicitor's Department publication "The Judge over your shoulder" (recommended reading)

"There are three "logical principles" to be followed in making a decision:

- to take into account all relevant considerations
- not to take into account an irrelevant consideration
- not to take a decision which is so unreasonable that no reasonable person properly directing himself could have taken it
- They are called the "Wednesbury principles", after the licensing case in which they were formulated.

Even if the decision-maker has followed the first and second principles, he may still have come to a decision which is so wildly unreasonable or perverse that it cannot have been within his discretion to make it, and it was therefore unlawful. He may have had before him all the relevant information and none that was irrelevant, but he may nonetheless have attached wholly disproportionate weight to a particular factor or made some other logical blunder, which turned his whole reasoning process awry."

RELEVANCE
The independent Barring Board will consider relevant conduct ("Harms, causes Harm, puts at risk of Harm or attempts or incites the Harm; has sexual material of children; sexually explicit images of violence or conduct of a sexual nature involving a child"). The full list is contained in Schedule 3 para 4 and para 10. SVGA 2006.

Guidance on relevance in Part V was limited to a consideration of whether a reasonable employer, when considering the risk of employing an applicant in a particular role, would find the information material to that decision.

The role of police is to identify whether the information would be relevant to either the IBB or employer when THEY (the IBB or employer) are considering the issue.

Differences in the Acts (Part V of the Police Act; Safeguarding Vulnerable Groups Act)
Part V made reference to regularly caring for, training, supervising or being in sole charge of Children/ Vulnerable Adults.
Safeguarding Vulnerable Groups Act (SVGA) examines 'regulated activity'.

Both Acts apply to people who are in roles or sectors with contact with Children (under 18) and Vulnerable people (vulnerable is defined in SVGA). You will have been notified which type of activity each application relates to.

Disclosure consideration (MP7b)
INFORMATION WHERE DISCLOSURE TO THE APPLICANT MAY NOT BE IN THE INTERESTS OF THE PREVENTION OR DETECTION OF CRIME.

Similar provisions apply in both Acts that prevents the disclosure of information to the applicant SVGA 24 9; Additional Info (Part V)

Whatever factors you decide are relevant, you need to be sure that the facts on which you base your decision are accurate and up to date.
You also need to be sure that the factors that influenced your decision are properly recorded - this is the purpose of the AT3: to provide an appropriate audit trail of your considerations and decisions.