DELETION OF RECORDS FROM NATIONAL POLICE SYSTEMS (PNC/NDNAD/IDENT1)

The process covering deletion requests for records held on national police systems in England and Wales.

This guidance outlines the national process for record deletion in respect of records held on the PNC, the National DNA Database (NDNAD) and the National Fingerprints Database (IDENT1)

Version 2.0

Foreword

The National Police Chiefs' Council (NPCC) has agreed to this revised strategy being circulated to, and adopted by, Police Forces in England & Wales.

It is NOT PROTECTIVELY MARKED under the Government Security Classifications and any referrals for advice and rationale in relation to Freedom of Information Act disclosure should be made to the National Police Freedom of Information and Data Protection Unit at npcc.foi.request@cru.pnn.police.uk

This revised strategy has been approved by the Information Management and Operational Requirements Coordination Committee (IMORCC). Guidelines/Strategy produced by the NPCC should be used by chief officers to shape police responses to ensure that the general public experience consistent levels of service. The operational implementation of all guidance and strategy will require operational choices to be made at local level in order to achieve the appropriate police response and this document should be used in conjunction with Authorised Professional Practice (APP) produced by the College of Policing. It will be updated and re-published as necessary.

Any queries relating to this document should be directed to the ACRO Criminal Records Office at deletions@acro.pnn.police.uk.

2018

Product Control Page

Author:	Jess Mullins	Records Management Supervisor
Address:	ACRO Criminal Records Office	💻 deletions@acro.pnn.police.uk

Contributors:	
Karen Progl (ACRO Criminal Records Office)	Robert Butlin (Home Office)
Stacey Dibbs (Metropolitan Police Service)	Carl Jennings (Home Office)
Various Police Forces	

Distribution List:	
All Police Forces (England & Wales)	Home Office (PNC Customer Support)
British Transport Police (BTP)	Home Office (Reconciliations Unit)
Ministry of Defence Police (MDP)	Forensic Information Databases Service
Service Police (Navy, Army & RAF)	Disclosure and Barring Service (DBS)
HM Revenue & Customs (HMRC)	Disclosure Scotland
Home Office (Identity Policy Unit)	Access Northern Ireland
Home Office (Police Live Services)	Information Commissioner's Office

Issue Control:		
Version	**Date**	**Details of Changes made to this report**
1.0	19th March 2015	Final version agreed.
1.1	19th May 2015	Various changes made to format and content.
1.2	12th May 2016	Various changes made to format and content.
1.3	10th January 2017	Various changes made to format and content.
1.4	27th July 2017	Various changes made to format and content.
1.5	3rd November 2017	New template adopted. New Appendix B and Appendix G incorporated. Updated Appeals process added.

Issue Control:		
Version	**Date**	**Details of Changes made to this report**
1.6	3rd January 2018	Various changes made to format and content following feedback from HO colleagues.
1.7	22nd June 2018	Various changes made to content following DPA 2018.
2.0	18th October 2018	Final version agreed.

INTENTIONALLY BLANK

Contents

1 Introduction

1.1 Purpose

1.1.1 This Guidance replaces both the 'Exceptional Case Procedure' as defined in the '*ACPO Retention Guidelines for Nominal Records on the Police National Computer*' issued in 2006, and the statutory guidance issued by the National DNA Database (NDNAD) Strategy Board on the destruction of DNA samples, DNA profiles and fingerprints issued in 2013.

1.1.2 The purpose of this Guidance is to ensure that a consistent approach is taken by relevant and specified Chief Officers[1] and others in relation to dealing with applications for the deletion of records from these three national police systems:

- Police National Computer (PNC)
- National DNA Database (NDNAD)
- National Fingerprint Database (IDENT1)

1.1.3 A full list of definitions in respect of terminology used throughout this Guidance can be found at Annex A.

1.2 Status

1.2.1 This Guidance is issued to Chief Officers in England & Wales by the NDNAD Strategy Board under section 63AB(2) of Police and Criminal Evidence Act 1984 ("PACE") as amended by the Protection of Freedoms Act 2012 ("PoFA"):

> (2) The National DNA Database Strategy Board must issue guidance about the destruction of DNA profiles which are, or may be, retained under this Part of the Act [Part V of the Police and Criminal Evidence Act 1984].
>
> (3) A Chief Officer of a police force in England and Wales must act in accordance with any guidance under subsection (2).

1.2.2 This Guidance has statutory effect only in relation to the destruction of DNA profiles, but, in the interests of expediency and consistency, this Guidance and the accompanying process applies equally to the deletion of DNA samples, fingerprints and PNC records as well as DNA profiles.

1.3 Scope

1.3.1 This Guidance only extends to records held on PNC, NDNAD and IDENT1. Records held locally by Chief Officers, whether stored on other electronic document management

[1] Specified Chief Officers are defined in s.63F s.11(a) Protection of Freedoms Act 2012.

systems or in manuscript, are managed by Chief Officers in accordance with the Authorised Professional Practice (APP) on Management of Police Information (MoPI)[2] published by the College of Policing.

1.3.2 For the avoidance of doubt this Guidance does not extend to the deletion of records held on the Police National Database.

1.3.3 Custody photographs will be considered by forces as part of the process at the same time that an applicant wishes to make an application in respect of records held on the PNC, IDENT1 and NDNAD.

1.3.4 However, applications which are solely in respect of a custody photograph will not be accepted under this process and if an applicant is seeking the removal of this one element, they will need to contact the force directly. The process for deletion of custody photographs is also covered in the Authorised Professional Practice (APP) on Management of Police Information (MoPI), which in turn refers to the Custody Image Review.

1.4 Record types and categories

1.4.1 Fingerprint records are held on IDENT1: DNA profiles on the NDNAD. Associated demographic information, which includes a person's name, address, descriptive details and relevant operational information, is held on the PNC.

1.4.2 PNC records can be created by any police force operating in any jurisdiction within the United Kingdom (UK) [3]or by any recognised Law Enforcement Agency (LEA) or Non-Police Prosecuting Agency (NPPA) with relevant permissions to do so, whether they are exercising their lawful duties within the UK or abroad e.g. the Royal Military Service Police.

1.4.3 Records held on the PNC show whether a person has ever been convicted[4] of a recordable offence or a non-recordable offence associated with a recordable offence.

1.4.4 A PNC record also contains information about non-conviction outcomes including 'Not Guilty' adjudications, 'acquittals', 'discontinuances' and 'No Further Action' (NFA) disposals. In this Guidance non-conviction outcomes are referred to as a person's 'Event History'.

1.4.5 The Criminal Justice Act 2003 amended PACE and provided the police with the power to take DNA samples and fingerprints without consent, from persons detained at a police station having been arrested for a recordable offence. Where such an arrest results in no

[2] https://www.app.college.police.uk/app-content/information-management/management-of-police-information/
[3] Jersey, Guernsey and the Isle of Man are Crown Dependencies and are not part of the UK but they do create records on the PNC.
[4] Under PACE 'conviction' includes both court convictions and 'non-court disposals' issued by the police, specifically cautions, conditional cautions, reprimands and warnings.

further action being taken, the person is referred to as a Criminal Justice arrestee - 'CJ Arrestee'.

1.5 Principles

1.5.1 The Government wants to protect the civil liberties of innocent citizens, whilst giving police the powers they need to identify suspects and solve crime using DNA and fingerprints (hereafter referred to as biometric information). The Government also recognises that there is a requirement for the police to hold certain information about an individual's criminal history for their policing purposes[5] and to satisfy the requirements of their criminal justice partners e.g. the courts. This information includes convictions, out of court disposals and other 'Event Histories'.

1.5.2 Police powers to take and retain DNA samples and fingerprints are set out in PACE. Changes to PACE were implemented through provisions contained in PoFA which include the requirement for the biological DNA sample obtained by the police to be immediately destroyed once the DNA profile has been obtained and no later than 6 months after it was taken, except in rare cases where it is needed as evidence for court. The length of time that an individual's biometric information can be retained depends on their conviction / 'Event History'.

1.5.3 PACE (as amended) allows the police to indefinitely retain the biometric information of individuals convicted of a recordable offence[6]. PACE also provides circumstances in which the police cannot retain the biometric information i.e. in regards to persons who are charged but not convicted of a 'Minor Offence' or arrested but not charged with a 'Qualifying Offence'. In both instances, the legislation requires the biometric information to be immediately deleted unless, in respect of the latter, an application to retain the biometric information is made to the Biometrics Commissioner under section 63G of PACE. However, the 'Event History' is retained on the PNC in accordance with the current retention policy outlined at 1.5.5.

1.5.4 Chief Officers are Controllers as defined by the Data Protection Act 2018 (DPA). They have the discretion in law to authorise the early deletion of records relating to legally retained biometric information, which they own on IDENT1 and NDNAD, but only where the grounds for so doing have been examined and agreed.

1.5.5 Under this Guidance, PNC records are required to be retained until a person is deemed to have reached 100 years of age. However, Chief Officers can exercise their discretion, in exceptional circumstances, to delete records for which they are responsible, specifically those relating to non-court disposals e.g. adult simple cautions and conditional cautions as well as any 'Event History' owned by them on the PNC but only where the grounds for so doing have been examined and agreed.

---

[5] As defined by the Code of Practice for the Management of Police Information (MoPI).

[6] An exception is made in respect of persons of less than 18 years subject to certain provisions being met.

1.5.6 Court convictions are not eligible for record deletion from the PNC under this process.

1.5.7 Where an offence is dealt with by way of a Penalty Notice for Disorder, that event will also be recorded on the PNC and it will form part of a person's 'Event History'. A person issued with a PND is not regarded as having a conviction.

1.5.8 A person may have an 'Event History' recorded on the PNC even though they have only come to the attention of the police, LEA or NPPA on one occasion and regardless of whether that one occasion resulted in the person being convicted of an offence.

2 Record Deletion Process

2.1 Overview

2.1.1 This Guidance sets out the process for making an application for the deletion of legally retained biometric information in circumstances described at 2.2.1 below, as well as making an application for the deletion of a PNC record or a specific arrest event held on a PNC record when the biometric information has already been deleted through automated processes or never obtained in the first instance and in respect of those instances where records are held due to an out of court disposal. This process is known as the 'Record Deletion Process' (hereafter referred to as the RDP).

2.2 Deletion of biometric information and associated PNC record

2.2.1 This Guidance firstly provides that individuals, in certain circumstances, may apply to have their lawfully retained biometric information deleted from national police systems (NDNAD and IDENT1) earlier than the periods specified under PACE (as amended).

2.2.2 These circumstances are as follows:

a. They have no previous convictions and their biometric information is held as a result of being arrested **and** charged with a Qualifying Offence but not subsequently convicted, which applies a 3 year biometric retention period under PoFA: or,

b. They have no previous convictions and their biometric information is held due to a PND, which applies a 2 year biometric retention period under PoFA.

2.2.3 In the above 2 circumstances, an individual can make an application under the RDP in respect of their biometric information and the associated entry held on the PNC. An individual is encouraged to 'evidence' their grounds when making an application. Please refer to 5.3 for further information on grounds and supporting evidence.

2.3 Out of Court Disposals

2.3.1 An individual can also make an application for record deletion in respect of an out of court disposal – caution / warning / reprimand / youth caution / conditional caution / youth conditional caution.

2.3.2 Applications for the deletion of a conditional caution will not be considered if the conditions are still 'live'.

2.3.3 Under PACE a caution, warning and reprimand is regarded as a conviction and, unless the offence in question is an "excluded offence", the biometric information taken in respect of such a disposal is retained indefinitely under PoFA.

2.3.4 Therefore, an individual may make an application under the RDP in respect of their records held on PNC, IDENT1 and NDNAD.

2.3.5 However, the individual is encouraged to sufficiently 'evidence' the grounds under which they are submitting an application and only if those grounds are examined and accepted by the Chief Officer will the records be deleted. Please refer to 5.3 for further information on grounds and supporting evidence.

2.3.6 Attention is drawn to s.27(4) of PACE in respect of the recording of out of court disposals on the PNC.

2.3.7 http://www.legislation.gov.uk/ukpga/1984/60/section/27

2.4 Deletion of PNC record only

2.4.1 In addition to the circumstances described at paragraphs 2.2. and 2.3 above, applications for record deletion can also be made under the processes described in this Guidance even when the automated processes introduced to manage the PoFA requirements have already caused the deletion of a person's biometric information i.e. they were arrested and charged with a 'Minor Offence' or they were arrested but not charged with a 'Qualifying Offence' and no application was made to retain the biometric information.

2.4.2 However, it should not be assumed that just because the biometric information has fallen to deletion via automated processes that the Chief Officer will approve the removal of the PNC record also. The request for deletion presented by the applicant will still need to be examined and agreed.

2.4.3 Please refer to 5.3 for further information on grounds and supporting evidence.

3 Unlawful Arrest/Sampling or Mistaken Identity

3.1 Requirement to delete biometric information

3.1.1 If it is apparent that biometric information has been taken as a result of an unlawful arrest or an arrest based on mistaken identity or the original sampling was unlawful i.e. the suspect was not formally arrested in the first instance, Chief Officers must, with very limited exceptions, destroy the biometric information, whether the individual makes an application under the RDP or not. This requirement is set out under section 63D of PACE (as amended).

3.1.2 In this context, 'arrest based on mistaken identity' refers to circumstances whereby there was an error such as arresting the wrong "John Smith", notwithstanding that the arrest procedure itself was lawfully carried out.

3.1.3 Situations where the evidence against a suspect is ultimately inconclusive will **not** be seen as an arrest based on mistaken identity; these cases may instead fit one of the other 'grounds' specified at Annex B.

3.1.4 Whilst the requirement under section 63D of PACE does not extend to the PNC record forces should consider whether this is still required for a policing purpose.

3.2 Destruction of samples

3.2.1 The destruction of DNA samples is dealt with under section 63R of PACE (as amended):

(2) Samples to which this section applies must be destroyed if it appears to the responsible chief officer of police that:

(a) the taking of the samples was unlawful, or

(b) the samples were taken from a person in connection with that person's arrest and the arrest was unlawful or based on mistaken identity.

3.3 Destruction of DNA profiles and fingerprints

3.3.1 The destruction of DNA profiles and fingerprints is dealt with under section 63D of PACE (as amended):

(2) Fingerprints and DNA profiles to which this section applies ("section 63D material") must be destroyed if it appears to the responsible chief officer of police that:

(a) the taking of the fingerprint or, in the case of a DNA profile, the taking of the sample from which the DNA profile was derived, was unlawful, or

(b) the fingerprint was taken, or, in the case of a DNA profile, was derived from a sample taken, from a person in connection with that person's arrest and the arrest was unlawful or based on mistaken identity.

3.3.2 The deletion must occur as soon as the information comes to the Chief Officers' attention. An application for record deletion is not necessary in these circumstances.

4 ACRO Criminal Records Office

4.1 The role of ACRO

4.1.1 ACRO Criminal Records Office, operating under the National Police Chiefs' Council (NPCC), is a national unit that manages criminal record information on behalf of the Police Service.

4.1.2 The ACRO Information Management unit is a unit embedded within ACRO.

4.1.3 The ACRO Information Management unit, acting as Processor, manages record deletion requests as a service to members of the public, and they act as the conduit between applicants and individual police forces.

4.1.4 Whilst the ACRO Information Management unit may advise forces on the process and offer guidance in relation to national policy it is not the role of the ACRO Information Management unit / ACRO to make or challenge decisions made by an individual police force.

4.1.5 The decision on whether to retain or dispose of an offence added to PNC is the responsibility of the Chief Officer of the owning force, in their capacity as Controller.

4.1.6 Applications and enquiries in respect of this process should be directed to the following address;

Via email to: deletions@acro.pnn.police.uk

Via post to:

Information Management unit
ACRO
PO Box 481
Fareham
PO14 9FS

4.1.7 Due to the number of enquiries received by the ACRO Information Management unit, they are unable to routinely take direct telephone calls. However, if an applicant wishes to be contacted by telephone they can request this via the ACRO Customer Services Unit and agree a suitable time for a call back. A message will be passed on to the ACRO

Information Management unit who will contact the applicant and advise them further on how to apply for record deletion.

4.1.8 Please refer to 11.1.4 for further information on this.

4.2 The ACRO Information Management unit

4.2.1 The ACRO Information Management unit will seek to ensure that a consistent approach is applied to the administration of this process across the Police Service and by anyone else using the RDP. In this regard the ACRO Information Management unit will:

- Coordinate and deal centrally with all requests for record deletion made by applicants in respect of records owned by Chief Officers in England & Wales.
- Redirect applicants to other UK jurisdictions where necessary or appropriate.
- Contact the applicant where the grounds have not been fully 'evidenced' in respect of applications made for record deletion to give the applicant the opportunity to provide additional information to support their request if they so wished.
- Reject applications made in respect of any court conviction.
- Reject applications made in respect of a conditional discharge and an absolute discharge.
- Reject applications where an individual is still subject to ongoing enquiries
- Reject applications which are regarded as a data dispute.
- Forward applications to police forces and LEA as appropriate and manage responses.
- Provide advice to relevant Chief Officers when requested.
- Manage the deletion of records held on the PNC as directed by Chief Officers.
- Manage the deletion of biometric information from NDNAD and IDENT1 as directed by Chief Officers.
- Advise forces once a record deletion is complete and where applicable, request the force to arrange for the deletion of the associated locally held fingerprints for approved applications.
- Act as an intermediary between the applicant and Chief Officers.
- Collate information on behalf of the Police Service for statistical purposes.

- Report to the Information Management and Operational Requirements Co-ordination Committee (IMORCC) as directed.
- Maintain a statistical record of decisions made by Chief Officers.

4.2.2 Although the ACRO Information Management unit may advise Chief Officers, when requested, as to whether a decision is consistent with determinations made in similar cases, the final decision will always rest with the Chief Officer who owns the relevant records. In this regard, it should be clear that the ACRO Information Management unit do not make the decisions on record deletion.

5 Process

5.1 Eligibility

5.1.1 The deletion of court convictions is outside the scope of this guidance. Individuals with a court conviction cannot apply to have their record deleted under the RDP from the Police National Computer.

5.1.2 Individuals must appeal against the conviction to the court if new evidence emerges and have 28 days within which to do so from the date of the court ruling.

5.1.3 Whilst a conditional discharge is not deemed to be a conviction unless the individual breaches the conditional discharge and is then re-sentenced, it is a guilty verdict established in Court and so such disposals will not be considered for deletion under this process. The same applies to an absolute discharge.

5.1.4 Where the investigation into an individual or court proceedings against them are ongoing, an individual cannot apply to have their records deleted because the full circumstances of their case might not be known at the time the application is made.

5.1.5 Where a record is shown on PNC as an impending prosecution this will not be sent to force until six months have elapsed since the date of arrest. This will then ensure that any administrative processes within police forces are complete. Such applications will be returned to the applicant to re-submit at a later date.

5.1.6 If the ACRO Information Management unit come across a record which contains an Impending Prosecution over six months old, the unit will liaise with the owning force to determine whether the case is still ongoing or whether it is just a matter of the record not being updated. If the latter applies, the ACRO Information Management unit will liaise with the relevant force requesting that the record is updated to reflect the outcome of the investigation.

5.1.7 Where an application is submitted less than six months after the arrest date and the outcome **is** recorded on PNC there is no reason not to send it to the relevant force if it meets the criteria set out in the guidance.

5.1.8 Individuals who are arrested but not convicted of a 'Minor Offence' and those arrested but not charged with a 'Qualifying Offence' will have their biometric information automatically deleted (provided certain other criteria are met), so there is no need to apply simply to have the associated biometric information deleted[7]. However, said individuals can make an application under the RDP to have the associated PNC entry reviewed under the process.

5.1.9 The term 'evidence' in the context of the Guidance simply means that individuals are encouraged to provide reasoning for why they feel their request for record deletion comes under the ground(s) that they have selected on the application form i.e. what happened for the individual to determine that their case falls under their chosen ground(s)?

5.1.10 Similarly, if an individual applies under the ground of Judicial Recommendation then any associated court transcripts should be provided within the application, where possible, to support the request which indicates that the Judge instructed that an individual's records should be deleted.

5.1.11 PoFA allows the police in certain circumstances to make applications to either the Biometrics Commissioner or a District Judge for the extended retention of an individual's biometric information (See Annex C). In such circumstances, applications made under the RDP will not be progressed until such time as the decision of the Biometrics Commissioner or District Judge is known. If the decision is made to approve the continued retention of the biometrics then the application for record deletion will be rejected.

5.1.12 Automated processes written into the PNC ensure the deletion of biometric information in accordance with the retention periods set out in PoFA (See Annex C). However, in all cases, unless an application is made under the RDP, the PNC record will be retained until the person to whom it relates is deemed to have reached 100 years of age.

5.1.13 Attached at Annex D is a table showing the circumstances in relation to which an application can be made under the RDP. These circumstances include where an application is being made for the early deletion of biometric information and circumstances when the biometric information has already been deleted by automated processes in accordance with the legislation and the applicant is seeking only the deletion of their PNC record. In all circumstances, the grounds for deletion must be clearly stated on the application.

[7] Information held on a PNC record can be ascertained though the submission of a subject access request.

5.1.14 Individuals who are seeking the deletion of records owned by Police Scotland or Police Service of Northern Ireland will need to contact those forces directly.

5.1.15 Individuals who claim that their personal data is wrongly held on someone else's record or that the information recorded on their own record is incorrect is regarded as a data dispute. As a result, all such disputes should be referred by the individual to the force concerned. This process does not cover the resolution of such matters and the ACRO Information Management unit will reject such requests.

5.2 Making an application

5.2.1 Individuals seeking the deletion of their biometric data and/or the deletion of a non-court disposal or 'Event History' from the PNC are encouraged to complete a formal application and state the grounds for having their records deleted. An electronic version of the application is available on the ACRO and gov.uk websites: hard copies will be provided on request.

5.2.2 In order to verify the identity of the person making a request for record deletion through reasonable means[8], the applicant should provide a copy of a **current** proof of identity which contains a full name, date of birth and current address. **The applicant should not send an original form of identity.**

5.2.3 A copy of a proof of identity can include passport, driving licence or similar document.

5.2.4 A copy of a proof of current address should be a full page official form of correspondence showing name and address (e.g. utility bill or bank statement) and dated within the last six months.

5.2.5 The ACRO Information Management unit must be satisfied that the documents provided by an individual sufficiently proves the applicant's identity. The Chief Officer reserves the right to request more information if they have doubts about the identity of the person making the request.

5.2.6 Further guidance on acceptable proofs of identity can be found on the ACRO website.

5.2.7 If original documents are not in English, in addition to supplying copies, applicants will also need to provide a translation in English.

5.2.8 Applicants must also indicate on the application how they wish to be contacted i.e. by post or by email.

5.2.9 Relevant contact information will then be provided to the Chief Officer of the force that owns the record(s) on the basis that if an email address is cited in the application as the primary method of contact, further communication with the applicant will be by email

[8] As outlined in Part 3 'Law Enforcement Processing' of the Data Protection Act 2018

and if a postal address is cited, further contact with the applicant will be by post[9].The ACRO Information Management unit will use the same preferred method of contact as applicable.

5.2.10 If the e-mail option is selected, the applicant should ensure that it is clearly written/ typed on Page 1 of the application form. If not, the ACRO Information Management unit will send any correspondence via post.

5.2.11 Please note that ACRO has a secure email address, but does not accept responsibility for the security of the email address of the applicant. By selecting this option the applicant accepts complete responsibility for this.

5.2.12 Likewise, the applicant is responsible for ensuring that the postal address provided is not one where correspondence is likely to be intercepted by a third party.

5.2.13 The applicant declaration page requires the box to be 'checked' by the individual applying for deletion to acknowledge the information outlined in the declaration on Page 5 of the application form.

5.2.14 Applications will only be considered if they originate from the individual concerned, their legal representative, a Member of Parliament or the appropriate adult where applicable.

5.2.15 Applicants who would like the ACRO Information Management unit or Police Force to contact some other person / organisation acting on their behalf in respect of their application (e.g. legal representative), will be required to submit a signed letter of authority with their application setting out the contact details of that person and providing explicit consent for their application to be discussed with that person / organisation.

5.2.16 The signed letter of authority must be dated within the last six months.

5.2.17 The ACRO Information Management unit will accept requests for deletion from a child (Under 18) providing that the ACRO Information Management unit or Police Force are satisfied that the child is capable of understanding their right to erasure and that the child has made the request freely. Responses will go back to the child directly as per the details provided on Page 1 the application form.

5.2.18 If the Police Force has any concerns about the child making the request then they reserve the right to engage the relevant adult as they see fit.

5.2.19 If an individual, such as a parent/legal guardian/appropriate adult, is looking to make a request on behalf of a child then a copy of a proof of identity and current address of the adult must also be included along with the required identity documents of the child.

[9] Normal considerations apply if the applicant makes direct contact with forces during the process.

5.2.20 Responses to requests made on behalf of the child will be sent to the address provided within the application form for the 'care of' the adult submitting the request.

5.2.21 In such instances, as per 5.2.13, there is also a check box on the applicant declaration page which the adult should select and date.

5.2.22 5.2.13, 5.2.18, 5.2.19, 5.2.20 also apply in those instances where an application is being made on behalf of a vulnerable adult.

5.2.23 If an individual is making an application on behalf of another adult in an official capacity, a copy of the relevant legal document (e.g. power of attorney) should be supplied where possible.

5.2.24 No fees are applicable for the service provided by the ACRO Information Management unit or by Chief Officers.

5.2.25 A Process Map covering the record deletion process is attached at Annex E.

5.3 Grounds and Supporting Evidence

5.3.1 On the whole, the basis for record deletion will be that an individual is no longer a suspect for the offence for which they were arrested or summonsed i.e. they have been eliminated from enquiries based on the grounds shown at Annex B. If this is so, the applicant is encouraged to make this clear in their application. The process entered into will thereafter validate any assertion made by the applicant i.e. that they had a proven alibi.

5.3.2 However, it is accepted that there will be exceptions to this, for example simple cautions. When an individual is issued with a caution they are presented with a declaration form and by signing this it confirms that the individual understands the consequences of accepting the simple caution that is being administered to them. Therefore, as there is an admittance of committing an offence the basis for a request for record deletion cannot be on the basis that the individual is no longer a suspect.

5.3.3 The submission of a record deletion application to the force should be treated as a MoPI review prompting forces to review all the information that they hold.

5.3.4 Examples of the grounds that Chief Officers are obliged to consider are provided at Annex B. The list is indicative not prescriptive, thus allowing Chief Officers to exercise professional judgment in deciding whether the early deletion of biometric information and the deletion of the associated PNC record is reasonable, based on all the information that is available to them.

5.3.5 If an applicant ticks a ground and the Chief Officer does not feel that this ground has been evidenced then it is best practice that forces review the remaining grounds to see if any of these apply instead.

5.3.6 In respect of any ground that an individual selects on the application form, the individual is encouraged to provide sufficient supporting information which in turn addresses the relevant ground applicable to their circumstances.

5.3.7 Whilst providing supporting information and circumstances surrounding the event sought for deletion is **not** a legal requirement, individuals are advised that providing such detail will enable a more thorough review to be carried out by the Chief Officer.

5.3.8 If more than one ground is chosen then the individual should ideally address each of these grounds in turn as this will further support the request for deletion.

5.3.9 However, forces will need to apply a practical approach when reviewing an application and so if an applicant ticks a number of grounds and has not explicitly addressed each one in turn, this is not a valid reason for rejecting an application for review if the applicant has still provided reasons for deletion.

5.3.10 Forces will always need to verify an applicant's version of events against what they hold locally and so if the information recorded on local systems does not support an applicant's assertions then this could impact the decision.

5.3.11 In respect of supporting 'evidence', individuals are encouraged to include:

- The offence/event that they are seeking to have deleted including any relevant information regarding date, time and location. This enables the ACRO Information Management unit and the force to verify the relevant entry sought for deletion.

- A full explanation of the circumstances of the arrest / event and the outcome of the investigation.

- The reason(s) why they feel that the records should be deleted from the PNC, NDNAD and IDENT1 systems. These reasons should, ideally, support the grounds selected on Page 2 of the application form.

5.3.12 As at 5.3.7, although it is not a mandatory requirement for individuals to provide the above supporting 'evidence' in respect of an application for record deletion this approach is recommended as it will support such a request.

5.3.13 If an individual chooses to supply any supporting documentation such as statements, NFA notices etc then they are welcome to do so.

5.3.14 Any supporting letters which may be written by the individual/witness/victim can also be submitted. However, individuals must be aware that such documentation may have little impact upon the outcome particularly in respect of submissions from witnesses/victims as forces have no way of knowing the circumstances under which these were created.

5.3.15 Provided an individual has sufficiently articulated a case for deleting their records from national police systems, and those reasons are examined and agreed by a Chief Officer, then the expectation will be that any records held on the NDNAD and IDENT 1 will be approved for deletion (where applicable) along with the PNC record. However, every request will be determined on a case-by-case basis by the owning force.

5.3.16 If records held on NDNAD and IDENT1 have already been deleted through the automated processes, then consideration need only be given by a Chief Officer to deleting the relevant PNC record – see 2.4. for further information on this circumstance.

5.3.17 Whilst there is no obligation to delete any legally retained records, a Chief Officer must have regard to the RDP and act in accordance with the Guidance issued by the NDNAD Strategy Board when making their decision.

5.3.18 It should be noted that the deletion of a record from the aforementioned systems is entirely at the discretion of the Chief Officer. Absent of a convincing argument as to why a record should be deleted means that the record will be retained in accordance with the current retention policy in place at the time. Once an application is received, the ACRO Information Management unit, through a check of the PNC, will first establish whether the individual is eligible to apply i.e. it may be that their biometric information has already been deleted through the automated processes built into national police systems or the application has been made in respect of the deletion of certain categories of records not covered by the RDP e.g. court convictions.

5.3.19 If the application meets the eligibility criteria, the ACRO Information Management unit will confirm whether the grounds for deletion have been sufficiently articulated by the applicant i.e. they are clear, unambiguous and appear credible. Applications that pass this threshold will be sent to the Chief Officer of the force that 'owns' the record(s) and the applicant advised accordingly. Applications that do not pass the threshold will be rejected.

5.3.20 In respect of individuals seeking the deletion of numerous arrest events, the RDP does not allow for a blanket approach to be applied, the process does not operate on the basis of 'delete one, delete all'.

5.3.21 If an individual is seeking the removal of more than one arrest event / numerous offences then this needs to be made clear in the application with the individual addressing each event in turn, providing the circumstances and reasons for why they wish for that event to be removed and the ground(s) under which they are applying for the removal of that particular event.

5.3.22 The application form provides the relevant separate pages to enable individuals to apply for the removal of more than one event from their PNC record.

5.3.23 The Chief Officer of the receiving force (in practice a person designated by the Chief Officer) will review the grounds presented in the application and consider any locally held records including;

a. Custody record.

b. Crime report.

c. PNC record.

And, if available or relevant:

d. MG3 report (Crown Prosecutor's advice on charging).

e. Investigating officer's report and/or follow up enquires.

f. Legal Services report.

g. IPCC investigation/Directorate of Professional Standards report.

h. Case file or other documentation may be required in complex cases.

6 Affecting Factors

6.1 No further action disposals

6.1.1 The reasons why in certain circumstances the police, LEA or NPPA decide to take 'No Further Action' (NFA) in particular cases are many and varied. Sometimes the NFA decision is made by the police or relevant investigating authority and at other times the decision is made by the Crown Prosecution Service (CPS) or relevant prosecuting authority.

6.1.2 This Guidance provides for applications to be made on the grounds shown at Annex B, e.g. 'No Crime' or 'Proven Alibi'. However, where cases result in an NFA outcome and, for the reasons above, it should not be concluded that such a case automatically falls under the grounds of 'No Crime'.

6.1.3 In this regard, it is not intended that the RDP should be used to challenge the retention of a record held on the PNC when an NFA decision has been made absent of the grounds shown at Annex B being sufficiently 'evidenced'.

6.1.4 If an individual has only NFA disposals on record then any fingerprints and DNA taken will be automatically disposed of in line with the provisions contained in PACE, as amended. However, the 'Event History' on PNC and whether that is retained or deleted remains solely at the discretion of the Chief Officer as outlined at 2.4.

6.2 Non-conviction outcomes at court

6.2.1 Acquittal at court, dismissal at court, or a conviction being overturned on appeal or by other judicial process, is not in itself grounds for record deletion as PACE allows biometric information to be lawfully retained for three years if an individual is charged with, but not convicted of, a Qualifying offence. Insufficient evidence to convict does not necessarily mean there is sufficient evidence for an individual to be eliminated as a suspect.

6.2.2 If an individual applies for the removal of a record in relation to a 'Not Guilty' outcome at Court then they are encouraged to clearly 'evidence' one of the grounds detailed in Annex B.

6.3 Event histories and further connected criminality

6.3.1 If an individual has been the subject of more than one arrest then the principle will apply that the early deletion of biometric information and deletion of a specific PNC record/arrest event will be determined by considering that person's complete 'Event History'.

6.3.2 Where concern of further connected criminality exists, the early deletion of biometric information and a PNC record will not be approved by a Chief Officer. This discretion only applies in relation to the early deletion of biometric information and PNC record.

6.3.3 The same discretion cannot be exercised in respect of biometric information which must be deleted in accordance with legislation albeit the PNC record may be retained e.g. in those instances where an individual has no previous convictions and their biometric information was taken in respect of an NFA.

6.4 Requirement for positive evidence

6.4.1 This Guidance is based on, though not limited to, a Chief Officer having substantial evidence that someone has been eliminated as a suspect before agreeing to delete their records. In this regard, a key consideration of a Chief Officer will be the nature of the incident that led to the arrest coupled with positive evidence that an individual has been eliminated as a suspect by the police, or relevant investigating agency, due, for instance, to mistaken identity or proven alibi.

6.4.2 Chief Officers must establish positive evidence that supports their decision to delete relevant records. For example, where a victim withdraws an allegation or no longer wishes to proceed, unless the allegation is malicious or false, it does not in itself provide the basis for record deletion. Likewise, insufficient evidence to charge or a case not proceeded with on a technical legal argument e.g. unlawful arrest, will not necessarily mean there is sufficient positive evidence for an individual to be eliminated as a suspect or automatically provide a basis for the deletion of their PNC record.

6.5 Retention of biometric information due to previous conviction

6.5.1 Initially, a Chief Officer may agree to the deletion of the biometric information in respect of the one event referenced in the application, but if the individual was arrested for a separate offence in relation to which no DNA was taken[10], the DNA profile from the first arrest event will be lawfully retained until investigations into that other arrest event have concluded. If the individual is subsequently convicted of an offence in respect of that other arrest event the biometric information that would otherwise have weeded will be retained until the person is deemed to have reached 100 years of age.

7 Role of the Controller

7.1 The Controller

7.1.1 When a force creates and updates records on the PNC in respect of their investigations then the Chief Officer is the Controller for that data; and as such they are responsible for ensuring that the data is lawfully managed.

7.1.2 When a force creates and updates records on the PNC on behalf of an NPPA then the Chief Officer is the Processor for that data.

7.1.3 If the ACRO Information Management unit receives a request for deletion in respect of an offence of an NPPA offence, then the force will need to liaise with the relevant agency in order to elicit a decision on record deletion.

7.1.4 Chief Officers should aim to respond in writing to the ACRO Information Management unit with their decision within one month of receiving the application. The time should be calculated from the day after the ACRO Information Management unit receives the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

7.1.5 If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month[11].

7.1.6 For practical purposes, this guidance adopts a 28-day period to ensure that compliance is within a calendar month.

7.1.7 Whilst the ACRO Information Management unit will process applications quickly (usually on the first working day of receipt), it should be noted that some forces exceed the aforementioned timeframe due to the volume of requests that they are processing.

---

[10] Possibly because it was originally taken in respect of the offence that the applicant is seeking to have deleted.
[11] Taken from https://ico.org.uk/for-organisations/guide-to-law-enforcement-processing-part-3-of-the-dp-act-2018/individual-rights/the-right-to-erasure-and-the-right-to-restriction/

7.1.8 Furthermore, if for whatever reason, the Chief Officer or the ACRO Information Management unit require additional information in order to progress a request for deletion, the 28-day period will not begin until a completed request for deletion is received.

7.1.9 There will also be instances where, due to the circumstances of the case, it will take a Chief Officer longer to assess the evidence and reach a decision. Chief Officers can extend the time to respond to an application by a further two months if the request is complex or if a number of requests have been received from the individual.

7.1.10 In these cases the receiving force should respond to the ACRO Information Management unit within one month to inform them of the status of the application and the reason for delay.

7.1.11 In such instances, the ACRO Information Management unit will contact the applicant and update them accordingly.

7.1.12 In respect of a decision, a template decision form is contained within Annex F and forces are encouraged to use this where possible to ensure that a consistent approach is adopted when responding to applicants.

7.1.13 If the application is agreed, the ACRO Information Management unit will manage the deletion of biometric information from national police systems (NDNAD and IDENT1) and the deletion of any associated records held on the PNC[12]. A template deletion request form will be used by the ACRO Information Management unit to request the deletion of the relevant records via the NDNAD Service Delivery Team, National Fingerprint Office (NFO) Integrity Team and Home Office Reconciliation Unit, where applicable. The ACRO Information Management unit will notify the applicant of the Chief Officer's decision.

7.1.14 Where a force decides to delete a PNC record but retain the record held at force level a record should be kept of the rationale for this decision in accordance with relevant retention schedules.

7.1.15 Where a force decides to delete a locally held record as a result of an approved record deletion application this should be managed in accordance with the Authorised Professional Practice (APP) on Management of Police Information (MoPI).

7.1.16 The ACRO Information Management unit should also be notified of a Chief Officer's decision not to delete relevant records from national police systems.

7.1.17 Chief Officers should provide reasons for their decision to retain the record(s) to the ACRO Information Management unit who in turn will share such information with the applicant.

[12] Deletions are to be carried out to the standards set by the Information Commissioner.

7.1.18 Not providing reasons, specifically in those cases where the information is being retained, is non-compliant with the rights extended to an individual under 'erasure or restriction of processing', outlined in Part 3 of the DPA.

7.1.19 When an application to delete records is not agreed by a Chief Officer the applicant should be made aware that their biometric information is being retained under PACE (as amended) and that the continued processing of their personal data is compliant with both PoFA and the DPA.

7.1.20 Similarly, the applicant will be informed if their biometric information is being retained on the basis that they have an impending prosecution or a previous conviction (e.g. in accordance with provisions contained under PACE, as amended).

7.1.21 It will be subject to local policy what rank of officer will be responsible for conducting an initial review of the application. Furthermore, the Chief Officer can delegate decision making where they see fit.

7.1.22 A parallel is drawn with the position set out in Statutory Disclosure Guidance[13] issued by the Home Office which defines 'Delegated Authority' as follows:

Principle 8 - Any delegation of the chief officer's responsibilities should be appropriate and fully documented

34. *The chief officer should consider whether any aspects of the decision making process are to be delegated. Any delegation should recognise the importance and complexity of the process and the chief officer should be satisfied that the officer to whom the delegation is made is entirely suitable for the task in terms of skills, training and experience. Where delegation occurs, the chief officer should ensure that the delegate has regard to this statutory guidance. Any decision to delegate should be documented and signed off by the chief officer.*

7.1.23 In this regard, the only criteria that needs to be considered is whether the officer to whom the delegation is made is entirely suitable for the task in terms of skills, training and experience therefore, it need not be someone of Chief Officer rank but should not drop below Inspector or police staff equivalent.

7.2 Force Deletions

7.2.1 There will be occasions when a force will need to manage the deletion of records outside of the RDP i.e. the need to delete records is not applicant driven, for instance:

I. The outcome of a PSD investigation is that relevant records relating to an individual need to be deleted from national police systems.

[13] www.gov.uk/government/uploads/system/uploads/attachment_data/file/452321/6_1155_HO_LW_Stat_Dis_Guide-v3.pdf

II. There is a court direction for a force to delete records held on national police systems.

III. Routine 'housekeeping' i.e. to ensure the accuracy of records therefore requires certain records to be deleted from national police systems.

7.2.2 In all of the above, and in all circumstances where the need to delete records does not stem from an application made under the RDP, then the deletion of records from national police systems should be managed by forces under existing processes through direct contact with the relevant database administrators . Such processes should also be used by forces in respect of the 'Disregarding Certain Convictions' procedure.

7.2.3 Forces can contact the ACRO Information Management unit for further advice if required.

8 Appeals

8.1 Overview

8.1.1 There is no formal appeals process with regards to challenging a decision made under the RDP.

8.1.2 However, applicants who wish to challenge an outcome should, in the first instance, formulate the representation that they wish to make in relation to the decision taken by the force to retain their record(s) and the ACRO Information Management unit will forward it to the originating force for their consideration.

8.1.3 Any such representations should be made as soon as feasibly possible or no later than 3 months once an applicant is in receipt of the decision following their initial application for record deletion.

8.1.4 Individuals are encouraged to set out their representation in a coherent and structured way and provide any 'evidence' that counters the decision made by the Chief Officer to retain the record.

8.1.5 The representation should also contain any further information or 'evidence' which was not previously provided with the application.

8.1.6 A submission of this nature will not be accepted if an individual simply disagrees with the decision that has been made, it should be properly evidenced.

8.1.7 Similarly, it is not the intention that this part of the process is used by an individual to have their investigation re-opened.

8.1.8 An appeal should be either e-mailed or posted to the ACRO Information Management unit who will refer this to the force accordingly.

8.1.9 The decision on whether or not to uphold an appeal should not be made by the same officer that made the original decision regarding retention.

8.1.10 Once a decision is received, the ACRO Information Management unit will advise the applicant of the outcome.

8.1.11 It is not possible to appeal an appeal decision, and if the ACRO Information Management unit or Chief Officer deems a request for deletion to be manifestly unfounded or excessive then the applicant will be advised as such.

8.1.12 However if there are exceptional circumstances where new information comes to light at a later date, that wasn't previously available to the applicant, this will be considered on a case by case basis by the relevant force to determine whether they wish to re-review the request.

8.2 Re-applying for record deletion

8.2.1 8.1.12 above also applies in those instances where an applicant submits a fresh application for record deletion in respect of the same event previously reviewed and decided upon under the RDP.

8.2.2 In such instances, the force will advise the ACRO Information Management unit whether they will accept the request and this will be determined based on factors such as the passage of time since the initial request for deletion, whether there is new information available and having due regard to the MoPI framework in respect of the local records which provide set review periods.

9 Complaints Procedure

9.1 Data Protection Officer (DPO)

9.1.1 Each force has a DPO responsible for the integrity of personal data held on force systems. If an individual believes that the information held about them is inaccurate, incomplete or is retained longer than necessary for a policing purpose they can write to the DPO. They will need to contact the force directly in order to do this.

9.2 Professional Standards Department (PSD)

9.2.1 Each force has a PSD; if an individual feels that a member of the police force has behaved in an unprofessional manner then they can write to them. They will need to contact the force directly in order to do this.

9.3 Information Commissioner's Office (ICO)

9.3.1 The ICO is the UK's independent body set up to uphold information rights. Their role is to uphold information rights in the public interest.

9.3.2 If an individual believes that a force is not complying with the DPA or other relevant legislation they can contact the ICO for advice or to raise a complaint in respect of a decision made under this process.

https://ico.org.uk/make-a-complaint/your-personal-information-concerns/

9.4 Judicial Review

9.4.1 An individual also has the right to seek judicial review if they wish to challenge a decision.

https://www.judiciary.gov.uk/you-and-the-judiciary/judicial-review/

9.5 Independent Office for Police Conduct (IOPC)

9.5.1 The IOPC oversees the police complaints system in England and Wales and sets the standards by which the police should handle complaints.

9.5.2 They are independent and make their decisions entirely independently of the police and government.

https://www.policeconduct.gov.uk/

9.6 ACRO

9.6.1 If an individual wishes to make a complaint in respect of the specific processes undertaken by the ACRO Information Management unit then this should be made in writing to the following address:

Senior Manager for National Services
ACRO
PO Box 481
Fareham
PO14 9FS

10 Accountability

10.1 Protecting personal information

10.1.1 A Privacy Impact Assessment has been undertaken and all procedures used in the RDP conform to relevant Information Assurance handling requirements.

10.1.2 All information provided by the applicant will be treated in the strictest confidence and will not be disclosed to any person or organisation not involved in the process without the express consent of the applicant.

10.1.3 The ACRO Information Management unit will share personal information with nominated points of contact in police forces, LEA, NPPA and the Home Office and with other parties as necessary for the purpose of processing an individual's application.

10.1.4 The ACRO Information Management unit may also use certain information (e.g. address and alias details) provided within an individual's application to update the PNC record in respect of certain cases where a request is rejected to ensure compliance with the 4th DPA principle.

10.1.5 The ACRO Information Management unit will retain all applications and correspondence with forces / relevant agencies for a period of 24 months.

10.1.6 This is usually when the applicant is advised of the Chief Officer's decision, but will be extended to include any follow up enquiries, appeals or complaints to the point at which they are resolved.

10.1.7 Applications and personal information will be deleted from the ACRO Information Management unit's electronic files after this period has elapsed.

10.1.8 Applicants are advised to keep safe all correspondence both sent and received as further copies will not be available once the information has been deleted by the ACRO Information Management unit.

10.2 Monitoring

10.2.1 The ACRO Information Management unit will monitor the deletion of records from the PNC and biometric information from NDNAD and IDENT1 to ensure that relevant processes are completed without delay.

10.3 Audit

10.3.1 The ACRO Information Management unit may be subject to annual audit by the NDNAD Strategy Board or as directed by IMORCC.

10.4 Annual Report

10.4.1 The NDNAD Strategy Board, under provisions contained in PoFA, is required to make an annual report to the Secretary of State for the Home Department about the exercise of its functions. RDP statistics will be used in the production of this report if called upon.

11 Communications

11.1 Forms and Guidance

11.1.1 The RDP application form and associated guidance is available on the ACRO website.

11.1.2 If an individual requires a copy of the guidance and application form to be posted they are to advise the ACRO Information Management unit via e-mail or by contacting the ACRO Customer Services team so that the unit can arrange for this.

11.1.3 Enquiries regarding this guidance should be directed in the first instance to the ACRO Deletions Mailbox: deletions@acro.pnn.police.uk

11.1.4 The ACRO Information Management unit do not routinely take direct telephone calls from the public, however, this does not prevent an individual from making a request for deletion over the telephone. By calling the ACRO Customer Services line, an individual will be advised on the steps they need to take in order to progress a request for record deletion which, will be through submission of an application form.

Telephone: +44(0)2380 479 920

11.1.5 If an update is sought on the status of an application then applicants should e-mail in to the ACRO Deletions Mailbox (deletions@acro.pnn.police.uk) and the unit will assist. However, the general rule is that if the ACRO Information Management unit have not contacted an applicant with a decision then this means that they are not yet in receipt of one from the force.

11.1.6 If applicants do not have access to e-mail and wish for further information or an update on their application, they can call the ACRO Customer Services line who will take a message for the ACRO Information Management unit who will then take the necessary action and contact the applicant back.

11.1.7 Please note that the ACRO Customer Services department cannot provide specific advice on the RDP nor are they able to provide an update on the status of an application.

INTENTIONALLY BLANK

Annex A – Definitions

The following terminology is used throughout this Guidance:

Biometric information – is the term that refers to the DNA profile and fingerprints, collectively referred to as section 63D material in PoFA.

Conviction – The act of being found guilty of an offence. Primarily this refers to a finding of Guilt at Court. However, under the Protection of Freedoms Act 2012 a conviction also includes cautions, warnings and reprimands which means that biometric information will be retained indefinitely. Cautions, warnings and reprimands are also known as 'Out of Court Disposals'.

Criminal Justice Arrestee (CJ Arrestee) – a person detained at a police station having been arrested for a recordable offence whose DNA samples and fingerprints are lawfully taken. Where such an arrest results in no further action being taken, the person is referred to as a Criminal Justice arrestee - 'CJ Arrestee'.

DNA Profile - A numerical representation of 13 specific points on a person's DNA which is developed from the biological sample originally provided. A DNA profile amounts to nothing more than a string of numbers.

DNA Sample – Any material that has come from a human body and consists of or includes human cells.

DPA – Data Protection Act 2018

Event History – refers to non-conviction outcomes held on the PNC.

Excluded Offence – is any recordable offence:

- That is not a 'Qualifying Offence' and
- The offence was committed when the person was under 18 years old and
- The person was not given a custodial sentence of more than 5 years and
- It is the only recordable offence of which the person has been convicted.

IDENT 1 – National Criminal Fingerprint Database.

Minor Offence – is any recordable offence that is not a 'Qualifying Offence'.

MoPI – Management of Police Information.

LEA – Law Enforcement Agency.

NDNAD – National DNA Database.

NFA – No Further Action police disposal.

NPPA – Non Police Prosecuting Agency.

Out of Court Disposal – Caution, Warning Reprimand, Youth Caution, Conditional Caution, Youth Conditional Caution.

PACE – Police and Criminal Evidence Act 1984.

PNC – Police National Computer.

PND – a Penalty Notice for Disorder (PND) is a one-off fine that can be issued on the spot to anyone over the age of 16. They are issued for low level anti-social and nuisance offending such as drunk and disorderly.

PoFA – Protection of Freedoms Act 2012.

Policing Purpose – relates to the investigation, detection and prevention of crime.

Qualifying Offence – currently there are over 400 'Qualifying Offences'. They are the more serious offences such as murder, manslaughter, rape, wounding, grievous bodily harm, assault occasioning actual bodily harm, robbery and burglary. Also included are numerous sex, indecency and firearms offences.

Recordable Offence – is an offence for which the police are required to keep a record. Generally speaking, these are crimes for which an individual could be sentenced to a term of imprisonment or they have otherwise been made recordable by statute. The term also includes a number of non-imprisonable offences for example begging and illegal taxi touting. The police are not able to take or retain the biometric information of an individual who is arrested for an offence which is not recordable.

Record Deletion Process (RDP) – is the process defined in this Guidance by which an individual can apply to have their biometric information and/or PNC records deleted from national police systems provided the grounds for doing so have been examined and agreed by a Chief Officer.

Annex B – Grounds for Record Deletion

There are no set criteria for the deletion of records e.g. “beyond reasonable doubt” or “balance of probabilities”; it is for Chief Officers to exercise professional judgment based on the information available.

Chief Officers will consider applications on an individual basis and will not set retention periods for groups of individuals, however defined.

The following are examples of circumstances in relation to which the deletion of biometric information and a person’s PNC record should be considered by a Chief Officer;

Unlawfully Taken The taking of fingerprints or a DNA sample from which the DNA profile was derived, was unlawful (i.e. if there was no arrest or the arrest was for a non-recordable offence.).

Mistaken Identity / Unlawful Arrest. The taking of fingerprints or a DNA profile which was derived from a sample taken from a person in connection with an arrest which was unlawful. Or, the arrest was based on mistaken identity. An ‘arrest based on mistaken identity’ refers to circumstances whereby there was an error such as arresting the wrong “John Smith”, notwithstanding that the arrest itself may still be lawful.

No Crime. Where it is established that a recordable crime has not been committed. For example, a sudden death where an individual is arrested at the scene and subsequently charged, but after post mortem it is determined that the deceased person died of natural causes and not as a result of homicide. It should be noted that being acquitted or found ‘Not Guilty’ at Court does not automatically mean that No Crime was committed as the CPS would have felt that there was enough evidence in the first instance to bring charges.

Malicious/False Allegation. Where the case against an individual has been withdrawn at any stage, and there is corroborative evidence that the case was based on a malicious or false allegation.

Proven Alibi. Where there is corroborative evidence that the individual has a proven alibi and as a result s/he is eliminated from the enquiry after being arrested.

Incorrect Disposal. Where disposal options are found to have been administered incorrectly, and under the correct disposal there would be no power to retain the DNA profile. In such circumstances, consideration should be given to deleting the DNA profile, fingerprints and the PNC record. Deletion in these circumstances could also be the product of review within the criminal justice process, for example, the withdrawal of a caution.

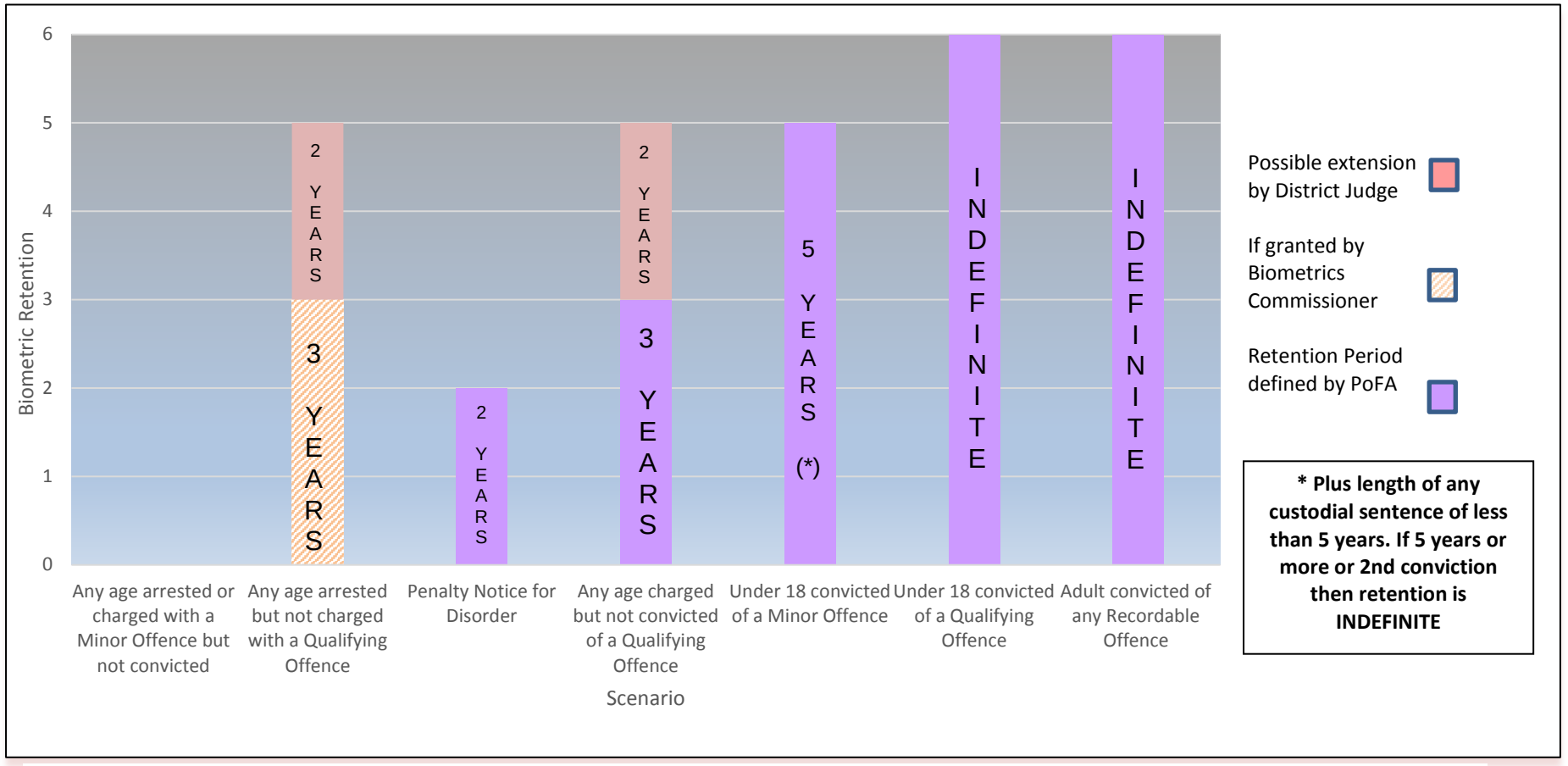
Suspect status not clear at the time of arrest. Where an individual is arrested at the outset of an enquiry, the distinction between the offender, victim and witness is not clear, and the individual is subsequently eliminated as a suspect (but may be a witness or victim).

Judicial Recommendation. If, in the course of court proceedings, a Magistrate or Judge makes a recommendation that an individual's DNA and fingerprints should be deleted. On such occasions, due consideration should be made in relation to the deletion of the PNC record.

Another person convicted of the offence. If there is the conviction of another person for the offence then the Chief Officer may wish to consider the deletion of the biometric information and PNC record, providing there is no possibility of there being more than one offender.

Public Interest. Where there is a wider public interest to do so. A Chief Officer must form an overall view on whether it would be in the public interest or not to retain the records in question based on all the information that is available to them. There would be a series of factors that Chief Officer would consider e.g. seriousness of the offence, level of culpability of the individual, whether the individual was under 18. Deletion of records from national police systems will not usually take place unless the Chief Officer is satisfied that there are Public Interest factors tending against retention outweigh those tending in favour.

Annex C – Retention Periods for Biometric Information (Fingerprints and DNA)



Note 1: The retention periods shown assumes that a person has no previous convictions and their biometric information is being held for no other reason

Note 2: The above table does NOT apply to the PNC record.

Annex D – Table of Circumstances and Eligibility

Ser	Disposal	Circumstance	Retention Period of Fingerprints and DNA	Eligibility of the Record Deletion Process			Comment
				DNA Profile	FP	PNC	
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
1	Court Conviction	Adult convicted at court of any recordable offence.	Indefinite retention.	No	No	No	Individuals can appeal against the conviction itself if new evidence emerges: https://www.gov.uk/appeal-against-sentence-conviction/magistrates-court-verdict
2	Court Conviction	Under 18 convicted at court of a qualifying offence.	Indefinite retention.	No	No	No	Individuals can appeal against the conviction itself if new evidence emerges: https://www.gov.uk/appeal-against-sentence-conviction/magistrates-court-verdict
3	Court Conviction	Under 18 convicted of a minor offence.	1st Conviction: 5 years (plus the length of any custodial sentence of less than 5 years), OR indefinite if the custodial sentence is 5 years or more	No	No	No	Individuals can appeal against the conviction itself if new evidence emerges: https://www.gov.uk/appeal-against-sentence-conviction/magistrates-court-verdict
			2nd Conviction: Indefinite retention.	No	No	No	Individuals can appeal against the conviction itself if new evidence emerges: https://www.gov.uk/appeal-against-sentence-conviction/magistrates-court-verdict

Ser	Disposal	Circumstance	Retention Period of Fingerprints and DNA	Eligibility of the Record Deletion Process			Comment
				DNA Profile	FP	PNC	
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
4	Out of Court Disposal	Adult awarded an 'Out of Court Disposal' for any recordable offence (adult simple caution or conditional caution).	Indefinite retention.	Yes	Yes	Yes	Individuals can use the Record Deletion Process to apply to have their records deleted from national police systems (NDNAD, IDENT1 and PNC) if they can evidence grounds that are agreed by a Chief Officer.
5	Out of Court Disposal	Under 18 awarded an 'Out of Court Disposal' in respect of a qualifying offence (youth caution, conditional caution, reprimand and final warning).	Indefinite retention.	Yes	Yes	Yes	Individuals can use the Record Deletion Process to apply to have their records deleted from national police systems (NDNAD, IDENT1 and PNC) if they can evidence grounds that are agreed by a Chief Officer.
6	Out of Court Disposal	Under 18 awarded an 'Out of Court Disposal' in respect of a minor offence (youth caution, conditional caution, reprimand and final warning) and no previous convictions on record.	5 year retention UNLESS there is a subsequent court conviction or out of court disposal on record before the end of the 5 year period. The presence of a subsequent conviction will then result in INDEFINITE retention.	Yes	Yes	Yes	Individuals can use the Record Deletion Process to apply to have their records deleted from national police systems (NDNAD, IDENT1 and PNC) if they can evidence grounds that are agreed by a Chief Officer.

Ser	Disposal	Circumstance	Retention Period of Fingerprints and DNA	Eligibility of the Record Deletion Process			Comment
				DNA Profile	FP	PNC	
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
7	Non-Conviction	Any age charged with but not convicted of a qualifying offence.	Automatic 3 year retention from date of samples.	Yes	Yes	Yes	S.63D material is automatically deleted from NDNAD and IDENT1 3 years from the date the case is resulted on the PNC. However, individuals can apply under the Record Deletion Process to have their s.63D material deleted earlier if they can evidence grounds that are agreed by a Chief Officer. A successful outcome will result in the deletion of the associated PNC entry.
8	Non-Conviction	Any age charged with but not convicted of a qualifying offence.	Automatic 3 year retention + 2 year extension granted by District Judge	No	No	No	S.63D material automatically deleted from NDNAD and IDENT1 at the expiry of the 3 year period unless an application is made to a District Judge to retain the material for a further 2 years. Individuals cannot use the Record Deletion Process to apply for record deletion during the 2 year period if an extension has been granted. See below.

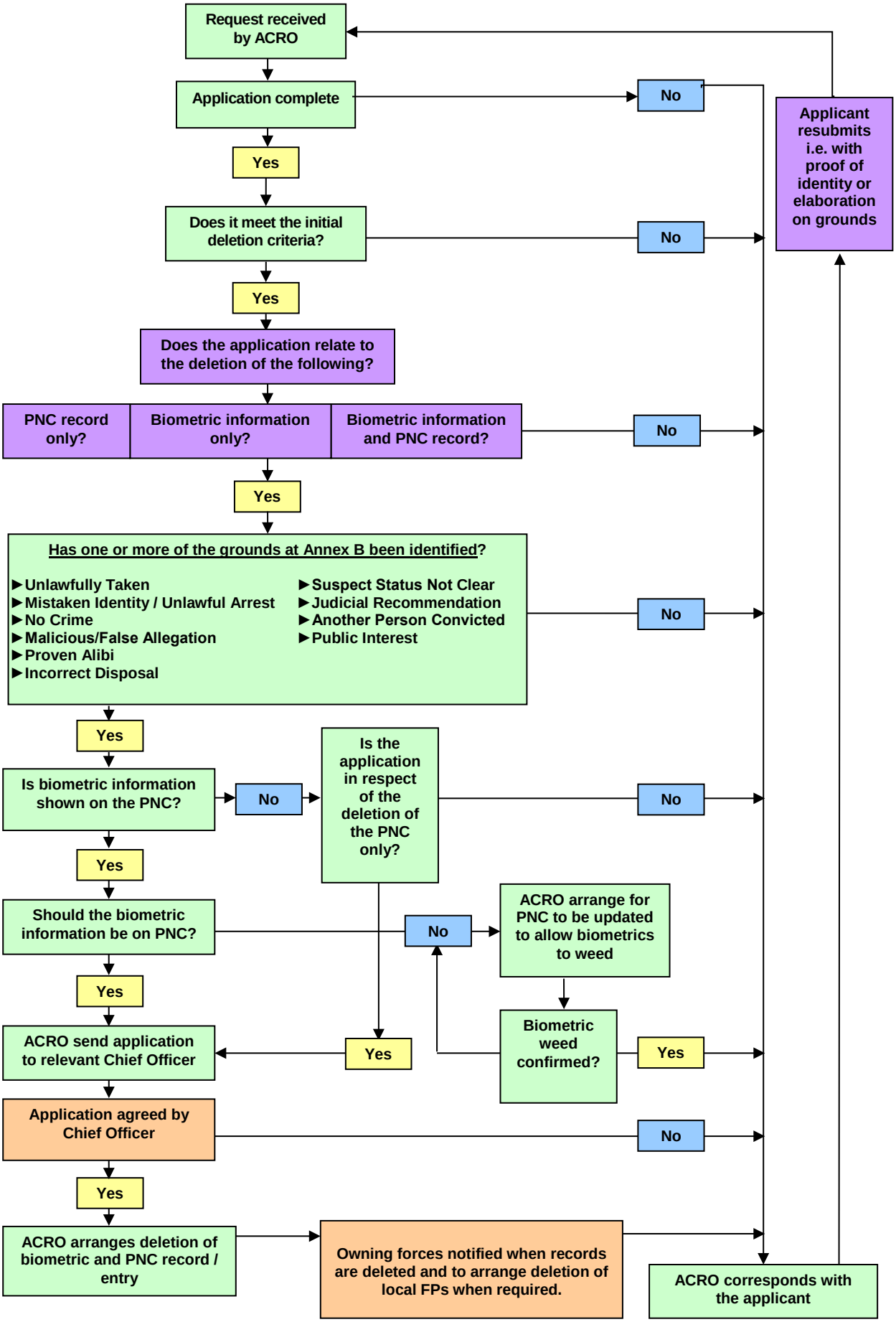
Ser	Disposal	Circumstance	Retention Period of Fingerprints and DNA	Eligibility of the Record Deletion Process			Comment
				DNA Profile	FP	PNC	
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
9	Non-Conviction	Any age charged with but not convicted of a qualifying offence.	Automatic 3 year retention + 2 year extension granted by District Judge	No	No	Yes	S.63D material is automatically deleted from NDNAD and IDENT1 at the expiry of the 2 year extension period. Individuals can use the Record Deletion Process to apply to have their PNC record deleted after the expiry of the 2 year period if they can evidence grounds that are agreed by a Chief Officer.
10	Non-Conviction	Any age arrested for but not charged with a qualifying offence.	Automatic deletion UNLESS 3 year extension is granted by the Biometrics Commissioner.	No	No	See (h)	S.63D material will be automatically deleted from NDNAD and IDENT1 as soon as the case is resulted on the PNC unless an application to retain the material is made to the Biometrics Commissioner. Individuals cannot use the Record Deletion Process to apply for record deletion once an extension of retention has been granted. If no extension is applied for, individuals can use the Record Deletion Process to apply to have the PNC record deleted.

Ser	Disposal	Circumstance	Retention Period of Fingerprints and DNA	Eligibility of the Record Deletion Process			Comment
				DNA Profile	FP	PNC	
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
11	Non-Conviction	Any age arrested for but not charged with a qualifying offence.	Initial 3 year extension granted by the Biometrics Commissioner + further 2 years granted by District Judge.	No	No	See (h)	S.63D material is automatically deleted from NDNAD and IDENT1 at the expiry of the 2 year extension period. Individuals cannot use the Record Deletion Process to apply for record deletion once an extension of retention has been granted by the District Judge. In such scenarios, individuals can use the Record Deletion Process to apply to have their PNC record deleted after the expiry of the 2 year period if they can evidence grounds that are agreed by a Chief Officer. If no extension is applied for, individuals can use the Record Deletion Process to apply to have the PNC record deleted.

Ser	Disposal	Circumstance	Retention Period of Fingerprints and DNA	Eligibility of the Record Deletion Process			Comment
				DNA Profile	FP	PNC	
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
12	Non-Conviction	Any age arrested, charged but found 'Not Guilty' of a minor offence.	None UNLESS there is a previous court conviction or out of court disposal on record. The presence of a previous conviction will then result in INDEFINITE retention of fingerprints and DNA.	See (h)	See (h)	Yes	S.63D material will be automatically deleted from NDNAD and IDENT1 as soon as the case is resulted on the PNC unless there is a previous conviction on record. The presence of a previous / subsequent conviction will retain the S.63D material taken in respect of the non-conviction. However, the record(s) may still eligible for review under the RDP.
13	Non-Conviction	Any age arrested, charged for a minor offence and given a Discontinuance.	6 month retention from court date UNLESS there is a previous court conviction or out of court disposal on record. The presence of a previous conviction will result in INDEFINITE retention.	See (h)	See (h)	Yes	S.63D material will be automatically deleted from NDNAD and IDENT1 at the expiry of the 6 month retention period. Unless there is a previous court conviction or out of court disposal on record. The presence of a previous / subsequent conviction will retain the S.63D material taken in respect of the non-conviction. However, the record(s) may still eligible for review under the RDP.

Ser	Disposal	Circumstance	Retention Period of Fingerprints and DNA	Eligibility of the Record Deletion Process			Comment
				DNA Profile	FP	PNC	
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
14	Non-Conviction	Any age arrested for but not charged with a minor offence, no previous convictions on record.	None	No	No	Yes	S.63D material deleted from NDNAD and IDENT1 as soon as the case is resulted on the PNC. Individuals can apply to have their PNC record deleted if they can evidence grounds that are agreed by a Chief Officer
15	Non-Conviction	Penalty Notice for Disorder (PND)	2 year retention from issuance.	Yes	Yes	Yes	S.63D material deleted from NDNAD and IDENT1 2 years from the date their case is resulted on the PNC. Individuals can have their s.63D material deleted early if they can evidence grounds that are agreed by a Chief Officer. A successful application will result in the deletion of the associated PNC entry. Alternatively, they can use the Record Deletion Process to apply to have their PND record deleted from the PNC after the expiry of the 2 year period if they can evidence grounds that are agreed by a Chief Officer.

Annex E – Process Map



Annex F – Force Decision Template

Nominal Information **ACRO Ref:** RD

Subject Name:

ASN:

PNC ID:

Outcome of application for deletion

Force Decision:

Grounds on which the application has been APPROVED/PARTIALLY APPROVED/REJECTED:

Additional/other grounds:

Refused - Rationale

Reason for application rejection (please enter below the rationale/justification for rejection):

☐ Please confirm that you are happy the above justification will be disclosed to the applicant

Approvals

If a deletion has been approved please confirm the records that are to be deleted:

If other please specify:

ACRO
Information Management unit
PO BOX 481
Fareham
PO14 9FS

Document Status & Version: Version 2.0
Version Date: 18th October 2018
Owned by: Information Management and Operational Requirements Coordination Committee