Standing up for kids

JUST FOR KIDS LAW

Police Records: A Guide for Professionals

October 2018

A guide to the organisations, guidance and laws that govern the keeping, sharing and use of police records held about an individual in England and Wales.

By
Alex Temple

Standing up for kids
JUST FOR KIDS LAW

October 2018

Contents

Foreword

From Enver Solomon: CEO at Just for Kids Law

Through my work in youth justice I've come to see how unforgiving the criminal records system can be for young people trying to move on from their past. Having a record that will never go away doesn't just block people from certain jobs; it can cause decades of stress and embarrassment long after any sentence has come to an end. This is neither proportionate nor just.

Just for Kids Law (**"JfKL"**) has worked for years to challenge the criminal records system and bring about meaningful reform. Recent successes in the courts have showed that change is possible. However, we're not there yet. Right now, we need to continue working in a system that is rigid, outdated and endlessly complicated.

This guide is intended to help any professionals attempting to navigate the criminal records system to advise individuals. It is also intended to help those wanting to challenge current systemic problems. I hope you find it useful. Please do contact us if you have feedback, want to work with us or need further advice.

Glossary of Terms

Term	Abbreviation	Definition	For full definition see:
Additional Verifiable Information	AVI	Information that comes to light after the recording of a crime, often with the purpose of proving one did not take place.	Section 3.1
Article 8		Refers to article 8 of the European Convention on Human Rights – the right to privacy.	Section 1.1
Audit Trail	AT	A document that records a disclosure decision in a standard format.	Section 5.5
Authorised Professional Practice guides	APP	A guide published by the College of Policing sets out how police forces are to keep, review and delete police information	Section 4.3
Criminal Records Check	CRC	A process by which the DBS check and disclose records of spent and unspent convictions that are not protected under the filtering rules.	Section 5.1
Code of Practice on the Management of Police Information	MoPI	Statutory guidance which impacts upon retention, disclosure and use of police records.	Section 2.0
Data Controller		An individual or organisation holding or processing information about a person. In this context, this will often be the police.	
Data Subject		An individual about whom a record is held.	
Enhanced Criminal Records Check	ECRC	A process by which the DBS check and disclose records of spent and unspent convictions that are not protected under the filtering rules. Also includes certain soft-intelligence held locally by police forces.	Section 5.1
Home Office Counting Rules	HOCR	A set of rules that dictates when incidents reported to the police are to be recorded as crimes.	Section 3.1
Information Commissioner's Office	ICO	Statutory body concerned with the regulation of personal data and a possible independent arbitrator of data protection concerns.	
Police National Computer	PNC	National data storage system maintained by the police. Contains various types of information, but does not contain "police information".	Section 1.6
Police National Database	PND	National data storage system that enables access of locally held "police information" to other police forces and some public agencies.	Section 1.6
Police records/criminal records		Information held about a person in relation to their interaction with the	Section 1.4

		police or criminal justice system or investigations relating to the same.	
Rehabilitation of Offenders Act 1974	ROA	Statute that sets out how convictions become "spent" and the result of this process.	Section 1.7
Spent conviction		A conviction that has exceeded the time specified in the ROA for the offender to be considered rehabilitated.	Section 1.7
Soft intelligence		Information that does not relate to convictions, cautions or other formal action taken by the police or criminal justice system.	Section 1.4
Unspent conviction		A conviction for which the offender is not yet considered to be rehabilitated under the ROA.	Section 1.7

1. Introduction

JfKL's youth justice lawyers have been working to improve the criminal records regime for young people, to help them move on from their past and leave childhood police records behind.

Through this work JfKL has reached two stark conclusions. The first is that this system of police records management is incredibly complex, involving a myriad of statute, case law and guidance that can make it difficult for individuals to know their rights and obligations. The second is that the amount of data processed as part of this system is massive. For example, the police hold around 52 million records of non-conviction information[1], and the Disclosure and Barring Service ("**DBS**") processes more than 5 million applications for criminal records checks annually[2]. Therefore, there is a clear need for advisors able to provide accurate guidance to people concerned about their police records.

JfKL produced this guide in order to assist practitioners to understand the legal framework, to advise clients and to successfully challenge unlawful data management decisions by the police and other organisations that have access to or hold police records.

The UK's records management scheme is fundamentally the same for adults and young people. Therefore, despite JfKL's work and expertise relating to children and young people, this guide covers the whole regime and is not limited to only the elements that exclusively effect young people.

How to use this guide

If you are unfamiliar with the records system, it is recommended that you start by reading the introductory chapter. It contains key definitions and provides some important context to elements of the system that are discussed in more detail throughout the guide.

However, if you are looking for more specific information on one element of the records management system, all the relevant cases and authorities are discussed under their relevant headings. You should be able to find the information you need by reference to the Contents or Glossary found above at pages 1 to 5.

1.1 What this document covers

This document covers the collection and keeping of records by the police, including the circumstances that will trigger a crime record being made and the time scales they are kept for. It also covers the process review and deletion of police records and the disclosure of records on Disclosure and Barring Service (**"DBS"**) Certificates. This document also covers the disclosure of information on "Police Certificates" issued for foreign travel and working abroad.

1.2 What this document does not cover

This document does not cover the management of biometric information or police photographs.

[1] The Guardian 21 August 2012: 'Has your information been stored on the Police National Database?'.

[2] See the section on the different CRC checks in this document at 18

This document does not cover the criminal record disclosure requirements for foreign travel or working abroad.

1.3 The meaning of "police records"

When this document uses the term "police records" or "criminal records" it is referring to information held about an individual on local and national police systems.

This includes convictions, cautions and warnings, which will be referred to as conviction information. It also includes "soft intelligence", which might also be referred to as police information or non-conviction information. In the 'Code of Practice on the Management of Police Information' (**"MoPI"**) this is referred to as "*all information including intelligence and personal data obtained and recorded for police purposes*[3] (emphasis added)".

This will include any Fixed Penalty Notices, Penalty Notices for Disorder, acquittals, other police intelligence (including allegations), cautions, reprimands and convictions. It can also include any convictions, warnings, reprimands and cautions of a person the applicant lives with[4]. It includes reports of crimes which did not lead to formal action. These records are known as no further action (**"NFA"**); or as "screened out" recordings[5]. They can be created for a range of reasons including a finding that there is no public interest to do proceed with a prosecution[6], insufficient evidence to secure conviction[7] or because the offender is too young or ill to be prosecuted[8]. In all of these cases, the information can still be considered for future disclosure[9].

MoPI defines police purposes as being:[10]

a. protecting life and property;
b. preserving order;
c. preventing the commission of offences;
d. bringing offenders to justice; and
e. any duty or responsibility of the police arising from common or statute law.

[3] Code of Practice on the Management of Police Information paragraph 2.2

[4] Unlock: the Information Hub. Disclosure of police intelligence on enhanced checks (approved information). http://hub.unlock.org.uk/knowledgebase/local-police-information-2/

[5] Metropolitan Police untitled Information Publication: https://www.met.police.uk/globalassets/foi-media/disclosure_2017/april_2017/information-rights-unit--information-regarding-the-process-of-screening-out-or-nfa-no-further-action-in-calendar-years-from-2014-to-february-2017

[6] Home Office Publication: Crime outcomes in England and Wales: year ending March 2016. Page 12. See Outcomes 9, 10 and 21.

[7] Ibid. See outcomes 13, 14, 15 and 16.

[8] Ibid. See outcomes 11 and 12.

[9] Standards and Compliance Unit guidance: Quality Assurance Framework: An applicant's introduction to the decision-making process for Enhanced Disclosure and Barring Service checks page 3, section titled "What kind of information can be considered for disclosure".

[10] Ibid paragraph 2.2.2

***Note that**: the rules that apply to conviction information are different for most purposes to non-conviction information. In addition, the rules that apply to records held on the Police National Computer* (**"PNC"**) *can differ to those on the Police National Database* (**"PND"**).

Where relevant, sections of this guide specify at the beginning whether they apply to conviction information, non-conviction information, or both.

1.4 The meaning of "management"

The "management" of police records refers to four distinct processes. Each one forms a part of the police records management system, but the rules that apply to each are different. They have each been the subject of legal challenges in recent years[11] as concepts that are distinct from one another. The 4 processes are:

1. *Retention:* this refers to the initial production of police records which takes place when the police produce records of investigations, suspicions and outcomes. This includes records entered into the PNC of cautions, convictions and other formal actions. It also refers to the keeping of records including when they are reviewed, updated and deleted from police systems.

2. *Disclosure by Criminal Records Check:* this refers to the sharing of police records with third parties such as employers, colleges and universities on official, issued documents. These include Criminal Records Certificates issued by the DBS and Police Certificates issued by ACRO.

3. *Self-Disclosure:* people can be required to volunteer details of their criminal record when applying for work, volunteer roles, courses of education and travel. This is called self-disclosure.

4. *Use:* decisions based on police information that has been shared or disclosed to a third party by whatever means are termed "use"[12]. Commonly, this will be a decision by an employer not to offer an applicant a job[13], to dismiss an employee, to refuse a student a place at a university or a decision to expel a student from a course[14].

[11] These are set out in each chapter to this guide, each of which is titled to correspond with one of the four processes.

[12] Ibid paragraph 13 stated as: "this case thus concerns the use made of the self-disclosure i.e. the decision to refuse to offer employment upon the basis of the disclosure".

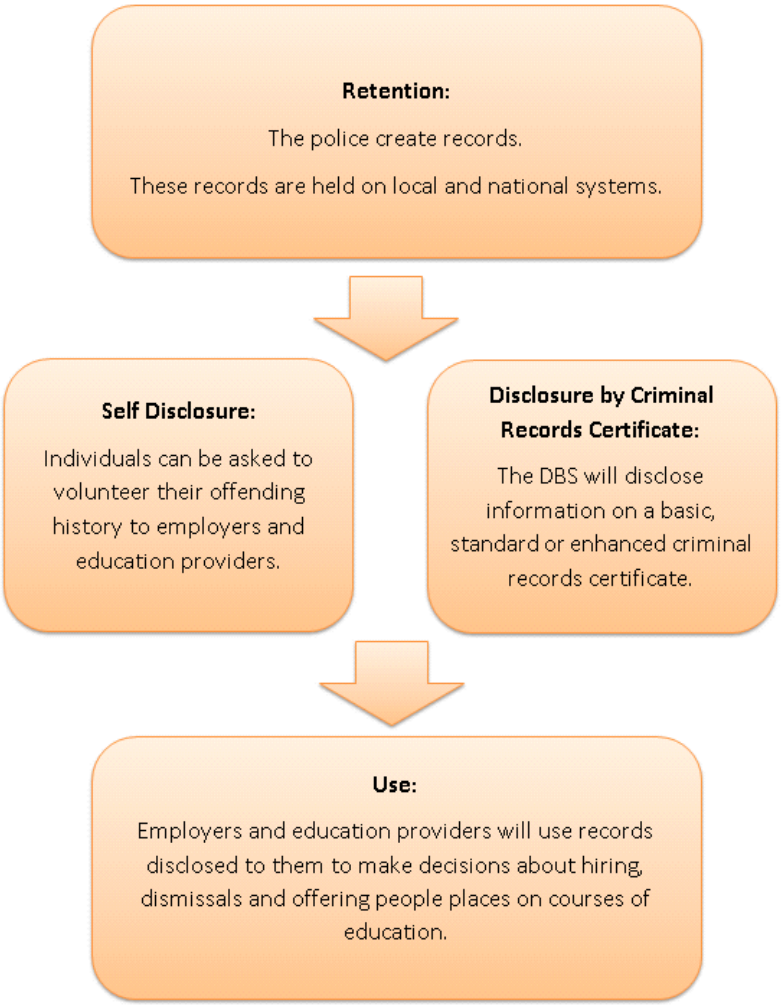
[13] Ibid

[14] HA v University of Wolverhampton & Ors (Rev 1) [2018] EWHC 144 (Admin). This case followed a decision to expel a student when the university discovered that he had two convictions that he had previously not disclosed.

This flow chart sets out the stages that exist in the criminal records management system.

Each step exists in law in isolation from the others, with their own rules.

This guide breaks down each stage by chapter, setting out the laws and regulations that apply to each individually.



1.5 Places where police records are kept

The Police National Computer

The Police National Computer (PNC) is a national database of police information[15]. It is accessible to police forces in England, Scotland, Wales, Northern Ireland, the Isle of Man and the Channel Islands. It is also accessible by the British Transport Police[16]. In addition, it shares information with a Europe-wide IT system called the Schengen Information System[17]. Other "non-police organisations" can, in some circumstances, also access the PNC. To obtain access, they must apply to a body called the

[15] Home Office guidance: Police National Computer (PNC). January 2014. Page 5. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/488515/PNC_v5.0_EXT_clean.pdf

[16] Ibid

[17] College of Policing information titled PNC – Police National Computer: http://www.college.police.uk/What-we-do/Learning/Professional-Training/Information-communication-technology/Pages/PNC-Police-National-Computer.aspx

Police Information Access Panel (PIAP)[18]. Some non-police organisations access the PNC through computer terminals installed in their premises. This is known as "direct access". Other non-police organisations obtain PNC information through a third party, usually a police force. This is known as "indirect access"[19]. A range of organisations have access to the PNC including G4S, Royal Mail, the Prison Service, the NHS and military branches[20].

The system contains[21]:

1. Personal descriptions;
2. Bail conditions;
3. Convictions;
4. Custodial history;
5. Wanted or missing reports;
6. Warning markers;
7. Pending prosecutions;
8. Disqualified driver records;
9. Cautions;
10. Drink drive related offences;
11. Reprimands; and
12. Formal warnings.

Police National Database

The Police National Database (PND) is similar to the PNC in that it enables police forces to share information electronically[22]. It is described as "a repository for copies of records which are held locally by forces[23]". The PND contains "details of allegations and/or investigations that did not result in an arrest[24]".

[18] HMIC Guidance "Use of the Police National Computer by non-police organisations". Dated May 2016 Page 3.

[19] Ibid

[20] Unlock InfoHub. Find a full list of organisations at: http://hub.unlock.org.uk/knowledgebase/organisations-access-police-national-computer-pnc/

[21] Home Office guidance: Police National Computer (PNC). January 2014. Pages 5 and 6 .

[22] National Policing Improvement Agency Code of Practice On the Operation and Use of the Police National Database dated March 2010. Page 2.

[23] Ibid page 6

[24] Solicitor Richard Easton writing for Sonn Macmillan Walker in September 2016. https://www.criminalsolicitor.co.uk/legal-guides/removal-of-information-held-on-the-police-national-computer-and-police-national-database/

The PND was created in the wake of the 2004 Bichard Inquiry Report.[25] This report followed the two murders of young people by Ian Huntley that were seen as resulting from a failure of the police to make information available to a school when he applied for employment.

The PND was originally protected with "confidential"[26] status under the Government Protective Marking Scheme. However, in 2014 the system in general was downgraded to "restricted", whilst certain pieces of information may retain the higher grading of protection.[27] This reduces the data protection standards that must be complied with by data handlers working with the PND.[28]

The PND is to be used "solely for police purposes[29]" although there is nothing in law to stop non-police organisations from accessing the PND if it supports these purposes[30]. The PND is available to all UK police forces and "wider criminal justice agencies"[31].

A privacy impact assessment was conducted of the PND and published in July 2018.[32] With regards to the organisations that presently have access, it states:

> "*The PND is currently available to policing organisations over the Public Sector Network for Policing (PSNP). This enables direct access for the 43 forces in England and Wales, Police Scotland, British Transport Police, Police Service of Northern Ireland, the Service Police Crime Bureau and the National Crime Agency. A limited number of officers in the Disclosure and Barring Service, Border Force, Immigration Enforcement, Identity & Passport Services, HMRC and the Security Industry Authority (SIA) also have access. The Medicines and Healthcare Products Regulatory Authority (MHRA) are in the process of on-boarding to PND at present. These organisations provide relevant intelligence information to PND and are granted access to the information on the system supplied by other user organisations*."

[25] National Law Enforcement Data Programme Law Enforcement Data Service (LEDS)– Privacy Impact Assessment Report. Published July 2018.

[26] Ibid paragraph 5.4

[27] Ibid

[28] See details of the varying obligations placed on each level of information in the Government Protective Marking Scheme Police document from Nottinghamshire Police; restricted is at paragraph 2.6 on page 6 and Confidential at 2.7 on page 7. https://www.nottinghamshire.police.uk/sites/default/files/documents/files/PS_171_GPMS_Policy.pdf

[29] National Policing Improvement Agency Code of Practice On the Operation and Use of the Police National Database dated March 2010. Guidance defines a police purpose as: 1. Protecting life and property; preserving order; preventing the commission of offences; bringing offenders to justice and any duty or responsibility of the police arising from common law or statute.

[30] Ibid page 7

[31] College of Policing Information: PND - Police National Database. http://www.college.police.uk/What-we-do/Learning/Professional-Training/Information-communication-technology/Pages/PND-Police-National-Database.aspx

[32] National Law Enforcement Data Programme Law Enforcement Data Service (LEDS)– Privacy Impact Assessment Report. Published July 2018.

Plans for Reform of the System: The National Law Enforcement Data Service

The National Law Enforcement Data Service (**"NLEDS"**) is a system that is intended to replace both the PND and the PNC with a single system[33]. At the time of writing, information about how this system will operate is limited, and there is no published timeline on the completion of the work, and when the PND and PNC will cease to operate.

1.6 Spent and Unspent Convictions

This section applies to conviction information.

Convictions can be either "spent" or "unspent". The 'Rehabilitation of Offenders Act 1974' ("**ROA**") contains a system by which convictions can become spent after certain periods of time[34]. Spent convictions are intended to cease having an effect on an individual's prospects of gaining access to employment or training[35], although the rules apply in limited circumstances[36] as exceptions to the ROA exist. The time taken for a conviction to become spent depends on the type of sentence.

The ROA states that: "*after the end of the rehabilitation period so applicable… that individual shall for the purposes of this Act be treated as a rehabilitated person* (emphasis added)"[37]. The effect of being a rehabilitated person is that they "*shall be treated for all purposes in law as a person who has not committed or been charged with or prosecuted for or convicted of or sentenced for the offence or offences which were the subject of that conviction*[38]". The table sets out the time after which a conviction becomes spent[39].

---

[33] National Law Enforcement Data Programme Law Enforcement Data Service (LEDS) – Privacy Impact Assessment Report. Published July 2018. See executive summary, section 1.

[34] Rehabilitation of Offenders Act 1974 s1.

[35] See DBS checks: guidance for employers published on 27 March 2013. Under heading 'Applicant's Rights': "The code of practice states that information on a DBS check should only be used in the context of a policy on the recruitment of ex-offenders. This is designed to protect applicants from unfair discrimination on the basis of non-relevant past convictions". https://www.gov.uk/guidance/dbs-check-requests-guidance-for-employers

[36] See information on the Rehabilitation of Offender's Act Exemptions Order at sections 5.2 in relation to CRC disclosure and 6.2 in relation to self-disclosure

[37] Rehabilitation of Offenders Act 1974 s1(1): "after the end of the rehabilitation period so applicable (including, where appropriate, any extension under section 6(4) below of the period originally applicable to the first-mentioned conviction) or, where that rehabilitation period ended before the commencement of this Act, after the commencement of this Act, that individual shall for the purposes of this Act be treated as a rehabilitated person in respect of the first-mentioned conviction and that conviction shall for those purposes be treated as spent."

[38] Ibid s4(1)

[39] Table rows 5-end taken from Nacro in March 2018. Page titled "Rehabilitation of Offenders Act". See: https://www.nacro.org.uk/resettlement-advice-service/support-for-individuals/disclosing-criminal-records/rehabilitation-offenders-act/#england

Rows 1 and 2 information taken from Ministry of Justice Guidance on the Rehabilitation of Offenders Act. Undated. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/216089/rehabilitation-offenders.pdf

Table rows 3 and 4 taken from Unlock Infohub

Sentence/disposal	Rehabilitation period for adults (aged 18 and over when convicted) from end of sentence including licence period	Rehabilitation period for young people (aged under 18 when convicted) from end of sentence including licence period
Reprimand, caution or final warning	Immediately	Immediately
Absolute discharge	Immediately	Immediately
Conditional discharge	At the end of the conditional period	At the end of the conditional period
A fine	1 year	1 year
Youth conditional caution	n/a	3 months
Community order or youth rehabilitation order+	Total length of order plus 1 year	Total length of order plus 6 months
Prison sentence or detention in a young offender institution for 6 months or less	Total length of sentence (including licence period) plus 2 years	Total length of sentence (including licence period) plus 18 months
Prison sentence or detention in a young offender institution for over 6 months and up to and including 30 months (2½ years)	Total length of sentence (including licence period) plus 4 years	Total length of sentence (including licence period) plus 2 years
Prison sentence or detention in a young offender institution for over 30 months (2½ years) and up to 48 months (4 years)	Total length of sentence (including licence period) plus 7 years	Total length of sentence (including licence period) plus 3½ years
Imprisonment or detention in a young offender institution for over 48 months (4 years) or a public protection sentence	Never spent	Never spent

The consequences for the management of records of convictions becoming spent is discussed in detail in each of the sections below. Note that this differs from "filtering" which is a process that "protects" cautions and convictions, removing them from automatic disclosure even when exemptions to the ROA apply. The Filtering Rules are discussed in the section numbered 5.6 "Home Office Rules".

1.7 Exemptions to the Rehabilitation of Offenders Act

This section applies to conviction information.

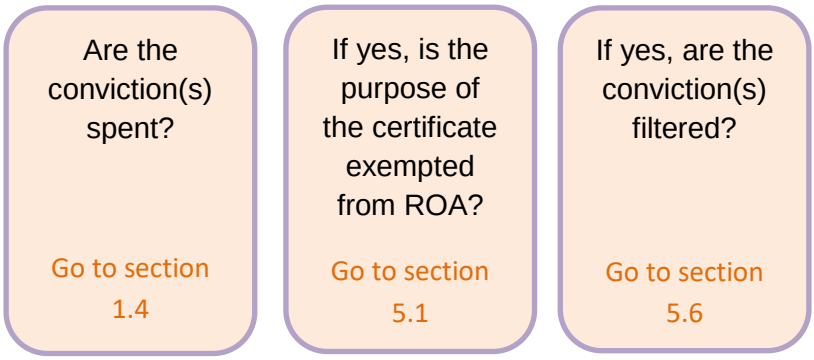
There are times when the ROA does not apply, and even spent convictions will automatically be disclosed unless "protected" under the filtering rules.

This occurs when the body requiring disclosure is asking an "exempted question". Bodies are empowered to do this when they are looking to fill a role which is exempt from the protections of the

ROA. These include: working with children and vulnerable people, working in healthcare, working in a role concerning national security, the legal professions, law enforcement, the Prison and Probation services, some employment in the financial sector and some licenced professions such as working with weapons or as a taxi driver[40]. A full list can be seen in section 5.1.

Some education providers can ask exempted questions when their course may involve access to vulnerable people, or where they provide accredited courses that may lead to one of the above employments[41].

The below flow diagram sets out which rules may apply, and where to find them in this document.



[40] Guidance on the Rehabilitation of Offenders Act 1974. Guidance dated 10 March 2014. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/299916/rehabilitation-of-offenders-guidance.pdf

[41] See HA v University of Wolverhampton at section 6.3

1.8 Article 8 of the European Convention on Human Rights

Article 8 ECHR ("**article 8**") is fundamental to the challenges that have been brought to the system of management of police records[42], and to the obligations of data controllers. It sets out that individuals have a right to privacy. It is broadly agreed that this right is infringed upon by the creation, retention, disclosure and use of criminal records[43]. However, state parties are granted a 'margin of appreciation' to derogate from this right when it is "*in accordance with the law*" and "*necessary in a democratic society*"[44]. The application of these tests in the courts, and how it is reflected in statute and guidance, is discussed in detail throughout this document.

Article 8 states that[45]:

> 1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
> 2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

1.9 The Code of Practice on Management of Police Information

This section applies to non-conviction information

The Code of Practice on the Management of Police Information (**"MoPI"**) is published by the Home Office[46] under statutory powers contained in the police acts of 1996[47] and 1997[48]. MOPI sets out the key principles to which the police must adhere when managing and processing information. MoPI also authorises further, more detailed authoritative guidance to be published to expand upon MoPI's principals. The latest guidance was published in October 2014 by the College of Policing and is found within the Management of Police Information section of its Authorised Professional Practice guide (**"APP"**)[49].

---

[42] Reference is made to article 8 throughout this document. Case digests in each chapter set out how the courts have applied this provision to the system of police records management.

[43] At 1.1 in this document.

[44] The Margin of Appreciation: Interpretation and Discretion Under The European Convention On Human Rights by Steven Greer. Dated July 2000 chapter 11.

[45] European Convention on Human Rights https://www.echr.coe.int/Documents/Convention_ENG.pdf

[46] Code of Practice on the Management of Police Information (MoPI)

[47] Sections 39 and 39A

[48] Sections 28.28A.73 and 73A

[49] https://www.app.college.police.uk/information-management-index/

The aim of MoPI is stated as ensuring consistency between police forces of procedures in relation to[50]:

1. obtaining and recording;
2. ensuring information is accurate;
3. reviewing and destroying information;
4. sharing between police and other agencies;
5. facilitating information sharing and the development of service-wide technological support for information management.

MoPI's provisions impact upon the creation, review, deletion and use of police information. The relevant provisions will therefore be set out in the sections to which they relate throughout this document.

[50] Code of Practice on the Management of Police Information (MoPI) paragraph 1.1.5

2. Retention

The retention of police information can be divided into two broad categories. These are covered separately in the following two chapters.

1. The creation of records;

2. The holding of records.

There are different rules regarding the creation and holding of records. There is a duty on police to create records of detected or reported crimes[51]. Courts have been willing to agree that the creation of police records is a justified interference with article 8 when done for a legitimate policing purpose[52].

However, the law prohibits the indiscriminate and indefinite holding of non-conviction police records[53]. There are also circumstances that allow for the deletion of convictions and cautions too, although these are limited. Different sets of rules apply to the review and deletion of records. The following sections on retention are therefore split into "Retention: Creation" and "Retention: Maintaining and Deleting Records".

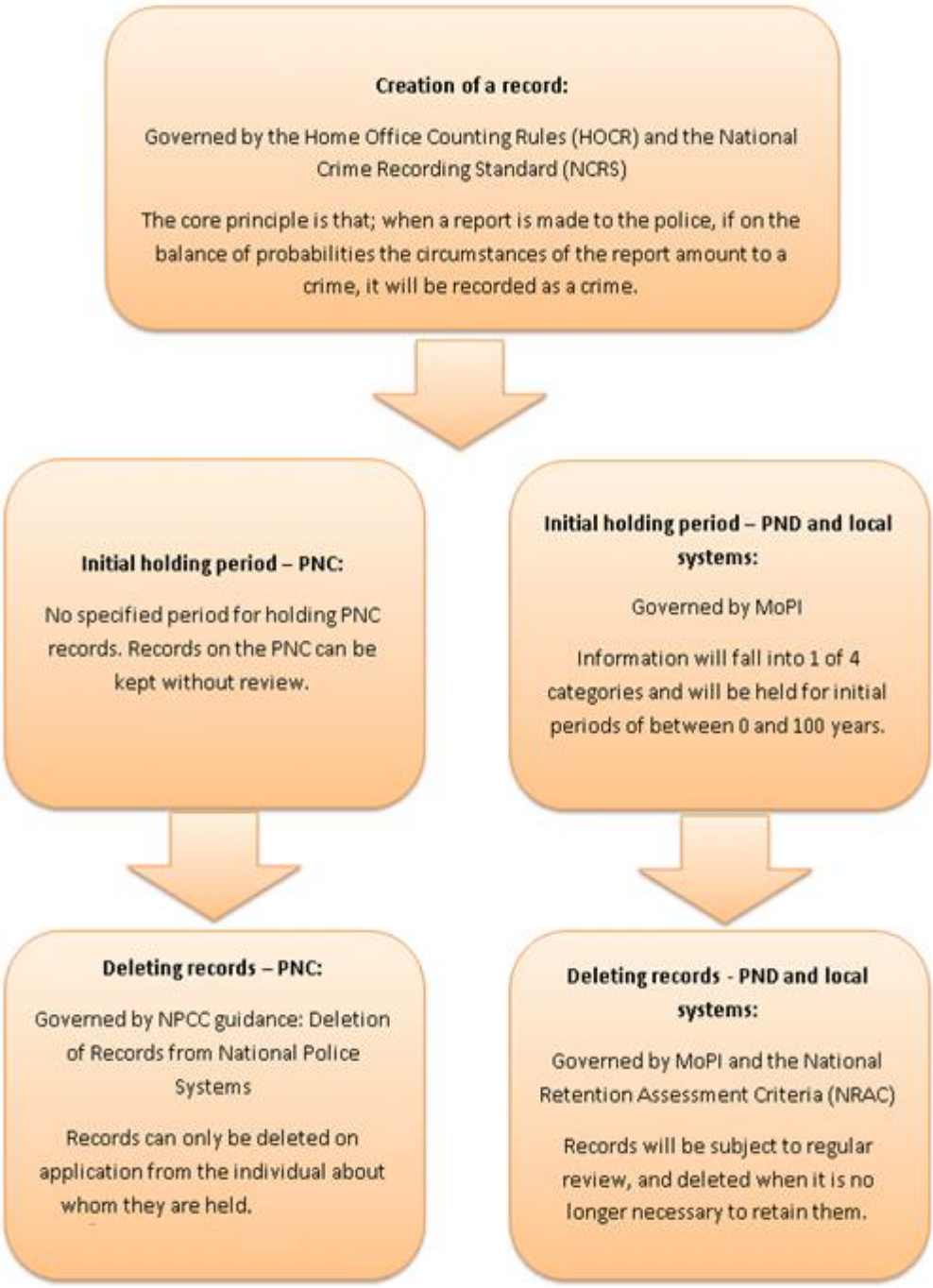
[51] See the section on the Home Office Counting Rules at section 3.1 of this document.

[52] See R (C) v Commissioner of the Police of the Metropolis at section 4.2 below.

[53] In the introduction to the Authorised Professional Practice it states that: "Retaining every piece of information collected is, however, impractical and unlawful". It is discussed throughout this guide that keeping crime records is an infringement of a person's article 8 rights and may only be done as long as it is "necessary" and "in accordance with the law". Similar expression is given at the rights of the data subject in the Data Protection Act 2018 at part 3 "Law Enforcement Processing".

The diagram to the right sets out how the key principals of retention fit into the process of making, keeping and deleting records that are described in detail in the following sections.

This diagram and the information in the following sections do not cover the management of biometric information or custody photographs.



3. Retention: Creation

This section covers:

1. *When can a crime record be created:* the **Home Office Counting Rules** stipulate when a crime must be recorded.

2. *What should a crime record look like:* the **National Crime Recording Standard** aims to standardise crime recording practices by setting out the key information a crime record will contain.

3.1 When can the police create records?

The Home Office maintains a policy of information gathering and retention within the UK's police forces[54]. It is claimed that records of reported incidents are needed to establish patterns of behaviour in individuals and populations, predict possible offending and protect the public[55].

The application of these policies is primarily expressed in the Home Office Counting Rules (**"HOCR"**) and the National Standard for Incident Recording (**"NSIR"**). Between them, these documents set out a broad duty for data collection by the police where events reported to the police are captured either as crimes, or as auditable incidents.

The Home Office Counting Rules

The HOCR are binding rules issued by the Home Office. They establish a duty on the police to record crimes. It is the primary set of rules for the creation of crime records and incorporates the National Crime Recording Standard (**"NCRS"**), which is intended to standardise the format of criminal records between forces[56]. A new version of the Counting Rules is issued each year by the Home Office.

The HOCR is made up of a main document called the 'Crime Recording General Rules'[57] (**"General Rules"**), together with a number of appendices which are intended to assist in interpretation of the main text.

[54] The Home Office document accompanying the Home Office Counting Rules titled "Vision and Purpose Statements for Crime Recording" states that: "That all police forces in England and Wales have the best crime recording system in the world: one that is consistently applied; delivers accurate statistics that are trusted by the public and puts the needs of victims at its core" and "The importance of [this document's] objectives, and in particular the need for the public and victims of crime to have confidence in the police response when they report a crime, makes it imperative that crimes are recorded consistently and accurately".

[55] JfKL have observed this argument being made in a number of litigations and pre-action correspondence with a number of police forces. It has also been stated as policy with police officials. In spirit it can be seen being advanced in the cases of Chief Constable of Humberside Police and others v The Information Commissioner [2009] and R (C) v Commissioner of Police of the Metropolis [2012].

[56] Description from the .gov website states "The aim of NCRS is to be victim focussed and maintain a consistent data set of recorded crime allegations across all forces."

[57] Home Office Counting Rules: Crime Recording General Rules April 2018
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/694432/count-general-apr-2018.pdf

The General Rules create a low threshold test for police to follow when establishing whether to record a crime[58].

A crime will be recorded when:

1. On the balance of probabilities, the circumstances reported to the police amount to a crime;
2. There is no credible evidence immediately available to show that a crime was not committed.

The box above sets the elements of the test that are common to all crimes[59]. At its simplest, this is the test the police are instructed to follow by the HOCR. However, it becomes more complicated when the type of offence, and the method through which it came to the police's attention, are considered. This is because crimes are split into two categories; 'victim related crimes', which are those that are committed against an individual victim, and 'crimes against the state', which are those that have no intended specific victim[60]. Which category an offence falls into is determined by the type of offence, regardless of the circumstances. The rules that apply to each differ, they are set out below.

Victim Related Offences

These will be recorded if, on the balance of probabilities, the police believe that the circumstances as reported by the victim amount to a crime and there is no information immediately available to contradict this.

A determination as to whether the circumstances constitute a crime should be made by the police on their knowledge of the law and the HOCR[61].

However, a belief held by the victim, or someone reasonably believed to be acting on the victim's behalf, that a crime has taken place will normally be enough to justify its recording as a crime.[62]

To trigger a recording, the incident must be reported by a victim or someone reasonably believed to be acting on the victim's behalf. This is known as "no victim – no crime".[63] There are exceptions to this rule that grant the police discretion to record a crime, even when there is no identifiable victim, when

[58] Ibid section A. "Whether & When to Record".

[59] For the purpose of identifying a common test, these rules have been paraphrased from the HOCR. The tests as they appear in the HOCR can be found in the main text in the first page of section A "Whether and When to Record".

[60] HOCR Section A (3 of 7): "Offences against the State are offences where the offence is made out notwithstanding the fact that the crime in question is not directed toward a specific intended victim".

[61] Ibid section A. "Whether & When to Record".

[62] HOCR General Rules paragraph 2.3

[63] HOCR General Rules Paragraphs 3.5 and 4.6

it is "appropriate or necessary to do so", or where the report comes from a third party with responsibility for the victim, such as a parent, carer or other professional[64].

Where a crime record is not produced, because no victim is identified, a "crime related incident" must still be recorded which can be amended to be a crime record if and when a victim is identified.[65]

Crimes Against the State

Crimes against the state will not necessarily have an identifiable victim. They must be recorded regardless of the circumstances in which they came to the attention of the police[66]. As with victim related offences, the police must make their determination based on their knowledge of the law and the HOCR.

As there is no victim in these offences to make a report, there is a different evidentiary standard that applies. The HOCR states that "for offences 'against the state' the points to prove to evidence the offence must clearly be made out before a crime is recorded"[67].

Any report not recorded as a crime will be recorded as an auditable incident[68]. All incidents reported to the police will result in a recording of a crime or incident.

Crimes in Schools

The HOCR contain a very narrow exemption to recording rules in the case of young people being reported for offences committed at school. This is called the Schools Protocol.[69]

Officers are instructed to encourage schools to deal with these matters under internal disciplinary procedures and should record the matter as an incident rather than a crime unless one of the following circumstances applies:

- the crime appears on the Schools Protocol serious offences annex to the HOCR[70];
- the school formally requests a record be made; or
- the child, their representative or guardian, request that a record be made.

The National Crime Recording Standard

The National Crime Recording Standard (**"NCRS"**) was adopted by all police forces in April 2002 with the aim of achieving consistency in the recording of crime and the introduction of a victim-oriented

[64] HOCR General Rules paragraph 3.6

[65] HOCR General Rules paragraph 3.5

[66] Ibid section A. "Recording State Based Offences"

[67] Ibid

[68] Ibid section A. "Crime Related Incidents".

[69] This is contained within the HOCR Section A.

[70] Ibid

approach to crime recording. Under principle 2.2 of the NCRS "*an incident will be recorded if, on the balance of probability, the circumstances of the victim's report amounts to a crime defined by law […] and there is no credible evidence to the contrary immediately available*". The NCRS requires police officers to determine this based on their knowledge of the law and the HOCR. This is an echo of the fundamental provisions of HOCR outlined above. NCRS states that unless additional verifiable information (**"AVI"**) is found to disprove the occurrence of the crime, the crime will remain on the record.

The final arbiter of the application and interpretation of the NCRS and HOCR is the crime registrar of the relevant police force[71]. A Crime Registrar "*is responsible for overseeing compliance with the crime recording process. He or she is the final arbiter for the force when deciding whether or not to record a crime or make a decision to cancel a crime[72]".* The Home Office Counting Rules direct the police that all *"Counting Rules enquiries should be directed to the Force Crime Registrar[73]"*.

The Code of Practice on the Management of Police Information (MoPI)

For an introduction to MoPI see section 1.9 of this document. MoPI sets out a duty for police to obtain and manage information[74]. It states that a duty exists on chief police officers "to obtain and manage information needed for a police purpose (emphasis added)". Note that police purposes are prescribed by MoPI and are listed at section 1.3 of this document.

The recording of "crime related incidents"

The National Standard for Incident Recording NSIR mandates that incidents reported to the police which are not recorded as crimes under the HOCR and MoPI should still be recorded and retained as crime related incidents. The NSIR states that the aim of this is safeguarding individuals and tackling anti-social behaviour[75]. It sets out the form and audit trail for reports recorded as incidents.

[71] Ibid

[72] Justice Inspectorates website. Page titled Crime-Recording Process': https://www.justiceinspectorates.gov.uk/hmicfrs/our-work/article/crime-data-integrity/crime-recording-process/. Note that according to this source the HOCR specifies that a Force Crime Registrar would not be in the normal chain of command, however the author could not find this provision in the source material.

[73] Home Office Counting Rules note contained in the footer of each page.

[74] MoPI Principal 4.1 on page 10

[75] The National Standard for Incident Recording 2011 Principal Aim.

3.2 What should a crime record look like?

The NCRS states that crime reports should record:

1. *Name;*
2. *Time, day, date of incident;*
3. *Time, day, date of recording;*
4. *How the crime was reported;*
5. *Who reported the crime and the method;*
6. *Location;*
7. *Modus operandi.*

Crime records must also conform to the standards set out in Data Protection Act 2018[76]. The Data Protection Act establishes 6 data protection principals in relation to criminal offence data.[77] The fourth data protection principal is relevant to the format of created crime records as it mandates that information recorded must be accurate and up to date[78].

Generally, crime records will incorporate an "action board" which sets out particulars of the incident being reported, actions taken by officers and their commentary and observations[79].

Under MoPI, when making records, the police should ensure that "the source of the information, the nature of the source, any assessment of the reliability of the source and any necessary restrictions on the use to be made of the information should be recorded to permit future review, reassessment and audit".[80]

Jargon: incidents recorded as a crime may be referred to as having been "crimed", and the process of making such records as "criming" incidents.

[76] The Information Commissioner's Website states on the page "Criminal Offence Data" that: "The Data Protection Act 2018 deals with this type of data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it".

[77] Data Protection Act 2018 Part 3 Chapter 2 sections 25 to 40.

[78] Data Protection Act 2018 Part 3 Chapter 2 s38

[79] This claim is based on Just for Kids Law's extensive experience in this field.

[80] Code of Practice on the Management of Police Information paragraph 4.3.2

4. Retention: Maintaining and Deleting Records

This section covers:

1. *How long the police are directed to keep police information for:* the Criminal Procedure and Investigation Act tells police to hold information for the length of an investigation or sentence. However, the **Authorised Professional Practice guides** set longer terms of retention. At the longest, these terms last until the data subject's 100th birthday.

2. *The quality standards that retained data should meet*: the **Data Protection Act** sets out that records must be acurate and up to date. This is echoed by the **Authorised Professional Practice guides.**

3. *How the police should review records*: records should be reviewed at regular intervals and assessed against the **National Retention Assessment Criteria**. Those that cannot be kept in line with the terms set out under the criteria should be deleted.

4. *How long to hold national records for:* the High Court has given the police broad powers to hold records on the Police National Computer indefinitely, even those that relate to minor offences. This is confirmed in the NPCC guide '**Deletion of Records from National Police Systems'**.

5. *Responding to requests to delete police information:* the **Authorised Professional Practice** guide sets out how police forces should respond to requests for deletion, in line with the retention criteria.

6. *Responding to requests to delete national records:* the NPCC guide '**Deletion of Records from National Police Systems'** sets out 8 narrow examples of circumstances in which police may exercise their discretion to delete information from from the PNC. The criteria offered in the guidance are not exhaustive and do not fetter the police's discretion.

The information to which the section applies:

1. ***Soft intelligence****:* the **Authorised Professional Practice guides, National Retention Assessment Criteria, Code of Practice on the Management of Police Information** and **Criminal Procedure and Investigations Act** apply exclusively to soft intelligence held by local forces and on the PND. This is because the rules around keeping and deleting these records are much more fluid and less clear cut than conviction information.
2. ***Conviction Information****:* the NPCC guide: **Deletion of Records from National Police Systems** applies to PNC information. It is therefore the only guidance in this section relevant to conviction information.

4.1 How long are the police directed to keep information for?

The law differs between conviction information and non-conviction information. It is also different again for biometric information.

Conviction information

The law relating to the holding of conviction information on the PNC has been relatively straightforward since the case of *Chief Constable of Humberside Police and others v The Information Commissioner [2009]*[81]*:*

> *Facts*
>
> Five Chief Constables appealed against the findings of the Information Tribunal and Information Commissioner ("**ITIC**"). The ITIC had ruled that the minor convictions of five individuals should be deleted from the PNC. In one of the five cases the individual had been assured that her relevant conviction, an official reprimand, would be removed from her record in accordance with a "weeding policy" then in force. This policy was subsequently changed, and the police view became that no convictions should be deleted except in exceptional circumstances[82].
>
> *Issue*
>
> The Court considered the retention of conviction information on the PNC, whether it was excessive to hold it indefinitely and whether it had been held for longer than necessary.
>
> *Decision*
>
> The Court of Appeal allowed the appeal of all applicants. The Court stated that "'*If the police say rationally and reasonably that convictions, however old or minor, have a value in the work they do, that should, in effect, be the end of the matter*". [83]

In effect, this case gives the police broad powers to keep conviction information on the PNC indefinitely, entirely under their own judgement of whether or not it is appropriate to do so. This was considered again in 2018 in *R (On the application of QSA) and others v Secretary of State for the Home Department and others [2018]*[84]:

[81] Chief Constable of Humberside Police, Chief Constable of Staffordshire Police, Chief Constable of Northumbria Police, Chief Constable of West Midlands Police, Chief Constable of Greater Manchester Police v The Information Commissioner [2009] EWCA Civ 1079

[82] Summary from 5RB Chambers: http://www.5rb.com/case/chief-constable-of-humberside-v-information-commissioner-another/

[83] Ibid paragraph 43

[84] R (On the application of QSA) and others v Secretary of State for the Home Department and others [2018] EWHC 407 (Admin)

Facts

The claimants were three women who had been groomed and sexually exploited as children and young adults. They each had multiple convictions for loitering or soliciting for the purposes of prostitution under the Street Offences Act 1959, s.1. They had largely been sentenced to financial penalties[85].

Issue

The court considered whether the information could be retained, or whether this considered a disproportionate interference with the applicants' Article 8 rights.

Decision

In relation to retention, the Court found that "*There is only a very limited interference with an individual's Article 8 rights when the State records and retains information about criminal convictions, and that limited interference is plainly justified in the public interest*"[86]. As such, the Court found no reason to grant relief in relation to the holding of records about a person's convictions. At the time of writing this case may be subject to an appeal once judgement is handed down in the case of P, G and W v Secretary of State for the Home Department. It should therefore be relied on with caution.

This case also considered issues of disclosure and is discussed again in section 5.3.

In spite of these cases, there is a process through which conviction information on the PNC can be removed. This is contained in the National Police Chiefs Council Deletion of Records from National Police Systems (**"DRNPS"**).

This guidance relates only to records held nationally on the PNC, and not to local records or those on the PND[87]. It has statutory status in relation to the deletion of DNA information only. It gives guidance to police chiefs on the deletion of other information held on the PNC[88] such as records of convictions, but this is not binding and there is no obligation for the police to have a system in place for the removal of records from the PNC.

[85] Summary on YJLC information page regarding this case. https://yjlc.uk/high-court-rules-childhood-criminal-records-disclosure-scheme-unlawful-again/

[86] Ibid paragraph 116

[87] Deletion Of Records From national Police Systems(PNC/NDNAD/IDENT1) version 1.1 paragraph 1.3.1

[88] Ibid paragraph 1.2.2

DRNPS sets out the following circumstances which would likely warrant the deletion of a PNC record once a request is received[89]:

1. Where it can be shown that no crime occurred;
2. Where is can be shown that the allegation against the applicant was malicious or false;
3. Where the applicant has been able to prove an alibi and they have been eliminated from the enquiry;
4. Where the police can be shown to have utilised an incorrect disposal, and the correct disposal would not have authorised the holding of the record on the PNC;
5. Where the individual was recorded onto the PNC because their status in relation to the crime (whether the suspect, victim or witness) was not known, but subsequently they were found not to be an offender;
6. When a judge or magistrate recommends the record's deletion as a part of their proceedings;
7. Where another person is subsequently convicted of the offence; or
8. Where there is a wider public interest in deleting the record.

The guidance makes clear that these are examples of circumstances which might warrant deletion, and that there are no set criteria. Instead, the guidance leaves this discretion to police chiefs, to be made upon the information available at the time[90].

This guidance replaced the "Exceptional Case Procedure" that had existed under ACPO[91].

Non-conviction information

What are the minimum timescales for keeping information?

The amount of time non-conviction information can be kept for is far more complex than conviction information. The best place to start is with the statutory provisions in the Criminal Procedure and Investigations Act 1996, which sets statutory minimum periods of retention and gives binding status to the Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice. This Code of Practice is concerned with gathering and retaining of information found in the course of police investigations and court proceedings. It relates to records held locally or on the PND[92]. It mandates that all materials which might be relevant may be stored and kept for the duration of any investigation and, if proceedings are brought, for the duration of the trial and any sentence[93].

[89] Ibid Annex A

[90] Ibid paragraphs 1-3.

[91] Ibid paragraph 1.1.1

[92] Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice March 2015 Preamble

[93] Ibid section 5. Duty to retain information.

However, the Authorised Professional Practice Guide states that its own minimum periods of retention will "far exceed" those imposed by the Criminal Procedure and Investigations Act. [94] Therefore, the Act will rarely have an impact on police decision making and has little relevance for the retention of non-conviction information.

When is there a discretion to delete information?

The Authorised Professional Practice guides, whilst having specified time periods for review of records and a maximum retention period of 100 years for information concerning the most serious offences[95], do not take a strictly prescriptive approach to the amount of time information should be kept for. Instead, the APP guides data controllers through merit-based assessments of information, to decide when to delete it.

The APP provides that information recorded for police purposes must be reviewed. Reviews either take place at regular, prescribed intervals as set out in MoPI[96]. These are known as "scheduled reviews". Alternately, they take place as "triggered reviews". These occur whenever a request for access to information is made. For example, when the DBS requests information to issue an ECRC, when another organisation asks for information about a data subject; or when the data subject themselves makes a Subject Access Request.[97]

APP divides offences into separate groups, each with different recommendations in relation to the frequency of reviews and the duration for which the information should be retained. In determining the categorisation of an offence, a police officer must take a risk-based approach and decide whether, after having considered the underlying offence to which the information relates, the individual represents a potentially dangerous person whose behaviour causes concern.

The categories are:

- *Group 1 – "certain public protection matters".*
    - Information in this category will be retained until the subject has reached 100 years of age.
    - Information in this category will be reviewed every 10 years to ensure that it is up to date.
    - Offences that have been amended by the Criminal Justice Act 2003 and are now considered serious specified offences under the that Act, should be retained as part of this group.

[94] Authorised Professional Practice Guide: Information management Retention, review and disposal. https://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#nrac-questions

[95] The APP no Retention, Review and Disposal states in relation to Group 1 information that, data "is placed within this group until a subject has reached 100 years of age". While this is vaguely worded and could mean that it is transferred to another group at 100 years, in Just for Kids Law's experience in litigating these issues it has been taken to mean that the information will not be kept beyond their 100th birthday.

[96] MOPI (2005), paragraph 4.6.1.

[97] APP on Retention, Review and Deletion, section headed "when should a triggered review take place".

- *Group 2 – "other sexual, violent or serious offences".*
    - Information in this category should be reviewed 10 years after creation and a risk based decision made as to whether to retain it taken.
    - This group also includes all specified offences[98] that are not serious offences as defined in the Criminal Justice Act 2003[99].
    - For sexual, violent and serious offences not specified in the Criminal Justice Act, the information can *only* be retained as long as the individual about whom it is kept continues to be considered a threat by reference to the National Retention Assessment Criteria.
- *Group 3 – all other offences:*
    - Records that fall within this group do not necessarily have to be reviewed. Forces may opt to use a system of time-based, automatic disposal for classes of information in this group. (*note that these guides are being reviewed in light of DPA 2018. This act contains a right of data subjects not to be subject to automated decision making which may affect the rules of review in this group.)*
    - Records relating to people who are convicted, acquitted, charged, arrested, questioned or implicated for offending behaviour which does not fall within group 1 or group 2 are dealt with in group 3.

Group 4 – miscellaneous provision. These provisions are not relevant to the retention of offender details.

The High Court commented on the retention of non-conviction information on the PNC in the case of *R (C) v Commissioner of Police of the Metropolis [2012]*[100]. The Court was willing to refuse the Claimant's request to have non-conviction information removed from police systems and the Judge put this finding in broad terms.

Facts

The claimants applied for judicial review of decisions of the police force to retain data after they had been arrested on suspicion of:

- assault occasioning actual bodily harm (ABH) in relation to the first applicant. They were arrested when they were an adult; and
- rape allegedly committed by the second applicant who was 12 at the time of arrest.

The police had decided not to proceed with formal action against either applicant[101].

[98] Examples include false imprisonment, kidnapping and manslaughter as listed in schedule 15 of the Act.

[99] A full list of these offences is recorded on the Police National Legal Database

[100] R (C) v Commissioner of Police of the Metropolis [2012] EWHC 1681 (Admin), [2012]

[101] Summary from Westlaw https://login.westlaw.co.uk/maf/wluk/app/document?src=doc&linktype=ref&context=7&crumb-action=replace&docguid=IED245B20BCB911E19CB1AF7886685E88

Issue

The Court considered the retention of details of the arrests on the Police National Computer.

Decision

The court found in this case, in relation to a record held on the Police National Computer that, "*a PNC record that did not include the basic history of [the alleged offender's] involvement with the police would be an incomplete and potentially misleading record. Moreover, if a similar allegation were made against [the individual] in the future, it would be profoundly unsatisfactory if it fell to be considered without knowledge of the earlier allegation and the arrest and investigation to which it gave rise. I am satisfied that retention of this kind of information in the PNC record is justified on any view. If it engages article 8 at all, the interference with [the individual's] right to respect for his private life is small and is plainly proportionate*".

What factors must forces consider when reviewing information?

Under the Authorised Professional Practice Guide, police data controllers must consider the National Retention Assessment Criteria ("NRAC")[102].

The NRAC provides five principles in relation to retention.

1. the infringement of an individual's privacy caused by retaining their personal information must satisfy the proportionality test;
2. forces should be confident that any records they dispose of are no longer necessary for policing purposes;
3. there should be a consistent approach to the retention of police information;
4. records which are accurate, adequate, up to date and necessary for policing purposes should be held for a minimum of six years from the date of creation, helping to ensure that police forces have sufficient information to identify offending patterns over time, and to help guard against individuals' efforts to avoid detection for lengthy periods;
5. beyond the six-year period, there is a requirement to review whether it is still necessary to keep the record for a policing purpose. The review process specifies that police forces may retain records only for as long as they are necessary. (Note: t*he NRAC template provides guidance on establishing whether or not information is still needed for a policing purpose. A copy of this template is included at* ***Appendix 2*** *to this guide*).

[102] Authorised Professional Practice Guide updated 11 April 2018: Information management Retention, review and disposal section 1.4

The NRAC asks a series of questions of the data controller making the assessment. "Yes" answers to any of the questions should result in the information being retained and a further review being scheduled[103]. The questions are:

- is there evidence of a capacity to inflict serious harm?
- are there any concerns in relation to children or vulnerable adults?
- did the behaviour involve a breach of trust?
- is there evidence of established links or associations which might increase the risk of harm?
- are there concerns in relation to substance misuse?
- are there concerns that an individual's mental state might exacerbate risk?

If the information is retained, it should be insured that:

- records remain adequate and up to date;
- new information can be considered; and
- risks are still relevant.

The Data Protection Act 2018 (**"DPA18"**) replaced the Data Protection Act 1998 (**"DPA98"**).[104] It is also relevant to the review process as it contains its own safeguards on maintaining and ensuring the quality of information. The APP is currently under review in light of the coming into force of DPA18.[105]

It includes six data protection principals for the processing of personal data "for law enforcement purposes".[106]

Law enforcement purposes are defined as *"the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*".[107]

The relevant data protection principles for the retention of non-conviction information are:

1. The first data protection principal:
    a. That the processing of personal data must be lawful and fair.
    b. To fulfil the lawfulness requirement in the case of "sensitive" information, the processing must either be consented to by the data subject, or it must be done for "strictly necessary for the law enforcement purpose";

[103] Ibid section titled "National Retention Assessment Criteria"

[104] Data Protection Act 2018 s.44 "The Data Protection Act 1998 is repealed, with the exception of section 62and paragraphs 13, 15, 16, 18 and 19 of Schedule 15 (which amend other enactments)."

[105] This information was given to JfKL by the College of Policing.

[106] Ibid. Part 3: "Law Enforcement Processing"

[107] Ibid s.31

2. The third data protection principle:
    a. That "personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed".
3. The fourth data protection principle:
    a. That information should be accurate and "where necessary" kept up to date;
    b. Data controllers are directed to take all "reasonable steps" to ensure that "*personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes*".
4. The fifth data protection principle:
    a. that "*personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed*".
    b. Periodic reviews of information to ensure their continued need to be stored must be conducted within "appropriate time limits".

The DPA18 sets out rights of the data subject in relation to information about them that is being processed for law enforcement purposes. These include a right to rectification of information where it can be shown to be inaccurate or incomplete.[108]

Section 77 of the Freedom of Information Act 2000 makes it an offence to deliberately alter or erase records once an application for access to them has been made, in an effort to avoid having to disclose them. This means that police forces may have to disclose any records that they hold to the data subject, even if these records are inaccurate, excessive or otherwise contravene the DPA18.

The principals of MoPI relevant to the review, retention and deletion of information are[109]:

1. Review of police information:
    - Information must be reviewed at intervals prescribed by the guidance in the Authorised Professional Practice Guide set out in the section below this one.
    - At each review, the likelihood that the information will be used for police purposes should be taken into account. Chief Officers should ensure that this process is audited.
2. Retention and deletion of police information:
    - Information should only be deleted if:
        - The information has been shown to be inaccurate, in ways which cannot be dealt with by amending the record; or
        - It is no longer considered that the information is necessary for police purposes.

[108] Ibid s.46

[109] Ibid paragraph 4.1

Biometric Information

While this guide does not deal with the rules concerning biometric information, this case makes comments on the balance of individual article 8 rights, and police purposes in the context of an increasing capacity for states to capture information. This is relevant to intelligence outside of the biometric data.

S And Marper V. The United Kingdom [2008][110]

This case concerns the management of biometric information, which includes fingerprints and DNA samples.

Facts

The case concerned 2 appellants. The first was arrested aged 11 and charged with attempted robbery. His fingerprints and DNA samples were taken by the police. He was acquitted at trial. The second applicant was arrested in March 2001 and charged with harassment. The charge came about in the context of his relationship. He and his partner reconciled before the trail and the case was therefore discontinued. The applicant had still had his finger prints and DNA taken at the police station. Both applicants asked for their fingerprints and DNA samples to be destroyed, but in both cases the police refused[111].

Issue

The court considered the blanket retention on DNA and other biometric evidence. The court made their decision on the general interaction between the rights of an individual under article 8 and the rights and duties of authorities to hold information on suspected and found offenders. The Court observed that "*the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. In the Court's view, the strong consensus existing among the Contracting States in this respect is of considerable importance and narrows the margin of appreciation left to the respondent State in the assessment of the permissible limits of the interference with private life in this sphere. The Court considers that any State claiming a pioneer role in the development of new technologies holds a special responsibility for striking the right balance in this regard*[112]".

[110] Applications nos. 30562/04 and 30566/

[111] Justice.org: https://justice.org.uk/s-marper-v-uk-2008/

[112] Ibid paragraph 112

Decision

The Court held that the retention of the applicant's biometric information to be a violation of their article 8 rights.

The case resulted in a system of deletion of biometric information when an investigation does not result in an admission of or finding of guilt. The guide is produced by the National Police Chiefs' Council and it is titled the Deletion of Records From National Police Systems. This guidance is binding in the context of biometric information. However, biometric information is beyond the remit of this Professionals' Guide and it is therefore not discussed further here.

5. Disclosure (CRC)

This section covers:

1. *The laws that tell individuals, employers and other bodies when they can request a criminal records check:* there are four types of criminal records certificate (issued by the DBS). Each can only be requested in specific circumstances, commonly when someone applies for a specified job. Each type contains a different level of disclosure, from only unspent convictions at the basic level, to spent convictions and non-conviction information at the enhanced level.

2. *The laws that mandate what information applicants for a criminal records check have the right to access:* a complex series of laws set out what information can actually appear on a criminal records certificate. Convictions can be filtered out of a disclosure on a check in limited circumstances, police information can always be considered for disclosure on enhanced checks as long as it remains on police systems.

3. *When the police should disclose non-conviction information on a criminal records check:* the **Statutory Disclosure Guidance** and **Quality Assurance Framework** tell chief police officers how to deal with requests for information held locally about an applicant for a criminal records check.

4. *The cases that have been brought to challenge the disclosure regime:* a number of high profile challenges have been successfully brought in recent years. These have mainly looked at the Home Office Filtering Rules that prevent some convictions from being disclosed.

5. *Call for reform for childhood records*: there have been a number of calls for reforming the system of disclosure for youth criminal records. The Government has responded to the House of Commons Justice Committee on this issue to say that they will not take action without a Supreme Court judgement currently awaiting hearing in June 2018.

6. *Other police powers to share records:* the police have other statutory powers, and common law powers, to share information about a data subject.

5.1 Introduction to Disclosure by Criminal Records Check:

A criminal records check is a process by which the DBS release police records to data subjects and organisations.

There are only limited circumstances in which an individual can be confident that a record is not going to appear on an Enhanced Criminal Records Check (**"ECRC"**), and none in which they can know for sure. An ECRC is the most comprehensive form of criminal records check and make up the vast majority of all checks issued[113]. Around 3.8 million were issued between 2014-2015[114].

Unspent convictions, as well as 'unfiltered' convictions and cautions will be disclosed on standard and enhanced checks[115]. Convictions and cautions that have been "filtered" under the Home Office Filtering Rules will not automatically be included (only if added in by the police as described below). The filtering rules apply to a narrow category of records and, should an individual receive a second caution or conviction, filtered offences may become disclosable again. In addition to this, cautions and convictions that have been filtered out of an ECRC can be added back in by the police.[116] However, it is unclear how often this actually happens.

The filtering rules do not apply to non-conviction records. The disclosure of these will always be within the discretion of disclosure bodies at the time a request for issue of an enhanced criminal records check is made. The following table shows the roles which require each level of criminal records check[117].

Basic check	Standard check	Enhanced check
All employment positions	Applying for a security industry licence	Working directly with children and vulnerable adults
Government/civil service positions	Solicitor or barrister	Teacher
Working in airports	Accountant	Social Worker
Office work	Veterinary surgeon	NHS Professional
Hospitality industry	FCA Approved persons role	Carer
Retail, supermarkets	Football stewards	Taxi driving licences
Personal licence to sell alcohol	Traffic warden	
	Member of the Master of Locksmiths Association	

[113] See detailed information at section 5.1.

[114] The Queen (on the application of QSA) and others v Secretary of State for the Home Department and another [2018] EWHC 407 (Admin) paragraph 53

[115] See "filtering rules" section below and "unspent convictions" in introductory chapter.

[116] The Quality Assurance Framework MP5. See the section for MP5 in the overview document found: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/353036/QAF_v9_OV1_Overview_of_QAF_Process_September_2014.pdf

[117] Unlock Infohub: Eligibility for standard and enhanced checks. http://hub.unlock.org.uk/knowledgebase/eligibility-criminal-record-checks/

The High Court has also been willing to uphold the right of education providers to access this information when they are providing a course which[118]:

- involves work in industry that would require an equivalent check; or
- acts as a gatekeeper by being accredited by a professional body to administer courses that are a pre-requisite to a profession that requires one of the above checks.

Types of Criminal Records Check

1. Basic:

Eligibility of applicant: Individuals can request basic disclosure for themselves. Employers cannot request this check for an applicant[119].

Contents of disclosure: this check will *only* disclose unspent convictions[120]. This is the only form of disclosure not to include spent convictions.

How many are issued: These checks make up approximately 20% of the more than 5 million checks issued annually[121].

2. Standard:

Eligibility of applicant: Individuals and sole traders cannot apply for a standard check directly. They must apply though an employer registered with the DBS[122]. The role for which the individual has applied must be listed in the Rehabilitation of Offenders Act Exemptions Order's schedules[123]. See the table at section 1.7 for a list of these professions.

Contents of disclosure: A standard check is not bound by the terms of the Rehabilitation of Offenders Act in that both spent and unspent convictions will be included[124].

How many are issued: Standard checks make up around 5% of the more than 5 million checks issued annually[125].

---

[118] HA v University of Wolverhampton & Ors (Rev 1) [2018] EWHC 144 (Admin) paragraph 111

[119] Government published information: "Criminal record checks when you apply for a role". https://www.gov.uk/criminal-record-checks-apply-role

[120] Government published information: "Basic checks". https://www.gov.uk/government/publications/basic-checks

[121] Unlock information hub: http://hub.unlock.org.uk/knowledgebase/types-of-criminal-record-checks-v2/

[122] ibid

[123] DBS: A guide to eligibility for DBS checks v8.1–April 2016.

[124] Government published information: "Criminal record checks when you apply for a role". https://www.gov.uk/criminal-record-checks-apply-role

[125] Unlock information hub: http://hub.unlock.org.uk/knowledgebase/types-of-criminal-record-checks-v2/

3. Enhanced:

Eligibility of applicant: Individuals and sole traders cannot apply for an enhanced check directly. They must apply though an employer registered with the DBS[126]. The role for which the individual has applied must be one that is "prescribed" in regulations made under section 113B, of the Police Act 1997[127]. The majority of these positions include where there is frequent or intensive contact with children or vulnerable adults, e.g. teachers, doctors or social workers[128]. A full list of such professions can be seen at section 1.4.

Contents of disclosure: An enhanced check is not bound by the terms of the Rehabilitation of Offenders Act in that both spent and unspent convictions will be included[129]. It can also include any other information defined as "police information", that is considered relevant and that the police think "ought to be disclosed[130]".

An enhanced check can also disclose whether or not the applicant is listed as being barred from working with children or vulnerable adults[131]. This is called a 'barred list check'[132]. It will reveal whether the person is listed on either of two lists. One prevents individuals from working with children, and the other from working with vulnerable adults. It is an offence to employ someone in a role which involves contact with these groups if they appear on the relevant list.

How many are issued: enhanced (with and without barred list) checks make up around 75% of the more than 5 million checks issued annually[133].

[126] ibid

[127] s113B, Part V of the Police Act 1997. See also the Information Hub by Unlock: Enhanced Disclosure. http://hub.unlock.org.uk/knowledgebase/enhanced-check/

[128] Unlock infohub: http://hub.unlock.org.uk/knowledgebase/standard-check/

[129] Government published information: "Criminal record checks when you apply for a role". https://www.gov.uk/criminal-record-checks-apply-role

[130] Statutory Disclosure Guidance to Police Chief Officers. See detailed discussion at section 5.5

[131] DBS checks: guidance for employers. https://www.gov.uk/guidance/dbs-check-requests-guidance-for-employers

[132] Government published online information "Apply to check someone else's records" https://www.gov.uk/dbs-check-applicant-criminal-record

[133] Unlock information hub: http://hub.unlock.org.uk/knowledgebase/types-of-criminal-record-checks-v2/

The obligation to make disclosure

The obligation on the police to make disclosure when a request for a criminal records certificate is received is contained within the Police Act 1997.

- Section 113A[134] of the Police Act enables employers to obtain access to records when considering applications from potential employees for occupations and voluntary positions set out within the Act. The sections require the DBS to issue a check, when one is required for an application for employment listed in the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975. In such a situation the disclosing officer should release information of every "*relevant matter*".

- Section 113B(4) of the Act mandates that before issuing an enhanced criminal record check the Secretary of State must request that any relevant chief police officer provides any information which "*(a) the chief police officer reasonably believes to be relevant for the purpose described in the statement under subsection (2), and (b) in the chief police officer's opinion, ought to be included in the check*".

- A relevant matter is any conviction or caution (either spent or unspent), as well as any additional information the chief police officer believes to be relevant for the prescribed purpose.

Which convictions and cautions are disclosed?

Basic checks disclose nothing more or less than your unspent convictions. Basic checks will therefore not be discussed any further and further references in this chapter to "checks" or "certificates" refer to standard and enhanced checks, as both standard and enhanced checks follow the same rules in relation to disclosure of cautions and convictions.

The Rehabilitation of Offenders Act 1974 (**"ROA"**) stipulates that convictions and cautions (which, under section 135(5) Legal Aid Sentencing and Punishment of Offenders Act 2012 include reprimands and warnings) for criminal offences do not have to be disclosed insofar as they are "spent". A conviction becomes spent after specified periods depending upon the age of the offender at the time of conviction and the type of sentence imposed. A caution becomes spent as soon as it is administered, other than conditional cautions which are spent after three months[135]. See section 1.6 of this document for a full breakdown of how different sentences and out of court disposals spend.

However, the Rehabilitation of Offenders 1974 Act (Exceptions) Order 1975 (**"The Order"**) establishes "exceptions" to the Rehabilitation of Offenders Act by permitting, in certain circumstances, disclosure of convictions and cautions that are spent. The Order applies to both standard and enhanced checks.

[134] The Police Act 1997 (Criminal Record Checks: Relevant Matters) (Amendment) (England and Wales) Order 2013

[135] Paragraph 1 of Schedule 2 ROA 1974. See also the table in the introductory chapter at section 1.6.

Therefore, on such certificates, spent *and* unspent convictions and cautions will be disclosed on both standard and enhanced certificates unless they have been filtered.

Jargon: filtered convictions may also be referred to as "protected" convictions.

Filtering

The Home Office Filtering Rules (HOFR), created in 2013,[136] set out the process by which convictions and cautions can be removed from the certainty of disclosure on an enhanced check if they satisfy certain criteria. The requirements are slightly different for adults (18+) and children (17 and below).

However, it should be noted that the police do have the technical power to add filtered cautions and convictions back into an enhanced certificate[137].

An adult conviction will be filtered after 11 years if it is:[138]

- Their only conviction. This means that if there are multiple convictions, no matter when they were administered, even if they resulted from the same event, they will never be filtered. This is known as the multiple convictions rule.
- They were not sentenced to custody as a result; and
- It does not appear on the list of non-filterable offences. If it appears on this list, it will never be filtered. This is known as the serious offences rule.

The same rules apply for children except that the time elapsed before the conviction can be filtered is 5.5 years.

An adult caution will be filtered after 6 years if it:

- Does not appear on the list of non-filterable offences.

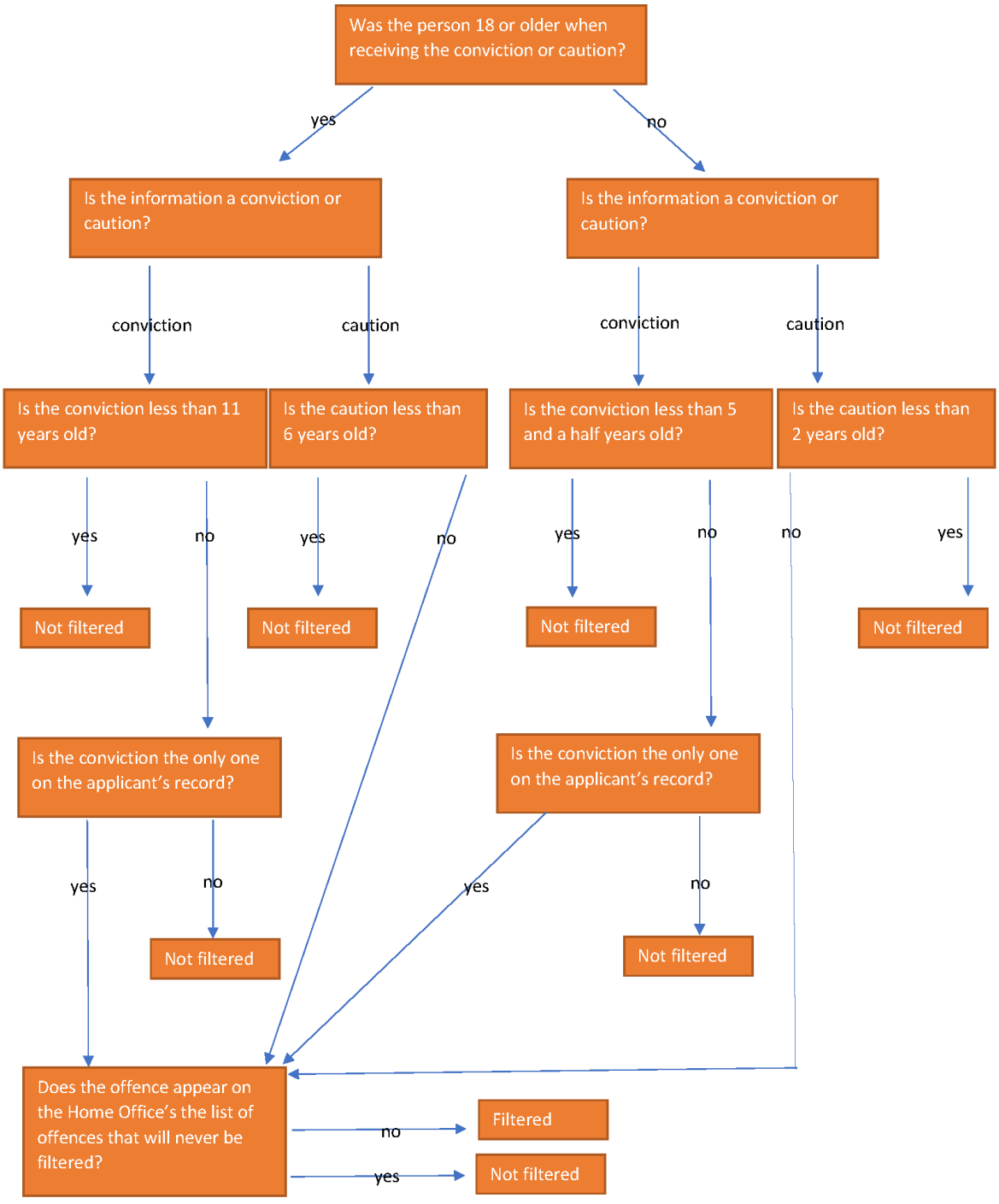
The same rules apply for children except that the time elapsed before the caution can be filtered is 2 years. The rules are set out in the flow chart.[139]

[136] Practical Law: New filtering rules for criminal record checks come into force. https://uk.practicallaw.thomsonreuters.com/3-530-5626?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

[137] The Quality Assurance Framework MP5. See the section for MP5 in the overview document found: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/353036/QAF_v9_OV1_Overview_of_QAF_Process_September_2014.pdf

[138] Government published guidance "Filtering rules for DBS certificates (criminal record checks)". (https://www.gov.uk/government/publications/filtering-rules-for-criminal-record-check-certificates/filtering-rules-for-dbs-certificates-criminal-record-checks).

[139] Information taken from Filtering rules for DBS checks (criminal record checks) published 17 December 2013. https://www.gov.uk/government/publications/filtering-rules-for-criminal-record-check-checks/filtering-rules-for-dbs-checks-criminal-record-checks


Was the person 18 or older when receiving the conviction or caution?
yes
no
Is the information a conviction or caution?
Is the information a conviction or caution?
conviction
caution
conviction
caution
Is the conviction less than 11 years old?
Is the caution less than 6 years old?
Is the conviction less than 5 and a half years old?
Is the caution less than 2 years old?
yes
no
yes
no
yes
no
no
yes
Not filtered
Not filtered
Not filtered
Not filtered
Is the conviction the only one on the applicant's record?
Is the conviction the only one on the applicant's record?
yes
no
yes
no
Not filtered
Not filtered
Does the offence appear on the Home Office's the list of offences that will never be filtered?
no
yes
Filtered
Not filtered

The filtering rules resulted from the case of *R (T) v Secretary of State for the Home Department [2014]*[140]*:*

Facts

"*T had received two police warnings when aged 11, in connection with the theft of bicycles. The warnings were revealed by an enhanced criminal record certificate (ECRC) when, aged 17, he applied for a job which involved working with children, and two years later when he applied to attend university.* [the Second Claimant] *had received a police caution when in her forties for leaving a shop with an unpaid-for item. She was unable to pursue a position as a carer when that caution was revealed by an ECRC. T and B claimed that the disclosure provisions were incompatible with their right to a private life under art.8. T also argued that the obligation to disclose the warnings was incompatible with art 8*[141]".

Issue

The Court considered whether the disclosures represented a justified interference with the applicant's article 8 rights.

Decision

The Supreme Court found that the regime governing disclosure of spent cautions was incompatible with the Claimant's right to privacy under article 8 as it was indiscriminate and, whilst the aim was legitimate, the indiscriminate nature of the requirement did not ensure that disclosure was necessary. This created an arbitrary interference with article 8[142]. The Court granted relief by issuing a declaration of incompatibility.

However, the filtering rules have themselves been criticized and are currently under challenge in *R (P and others) v Secretary of State for the Home Department [2017]*[143]*:*

Facts

The Claimants responded to an appeal form the Government over a successful High Court, and Court of Appeal challenge regarding rules that exempted the Claimants' cautions and convictions from becoming protected. *G* had been cautioned at age 12 for sexual activity with

[140] R (T) v Chief Constable of Greater Manchester Police; R (B) v Secretary of State for the Home Department [2015] AC 49

[141] Summary of facts taken from Westlaw case analysis: https://login.westlaw.co.uk/maf/wluk/app/document?src=doc&linktype=ref&context=16&crumb-action=replace&docguid=I18B68DC0F6D911E395D0BFCBF7868EC3

[142] Ibid paragraph 113

[143] R (on the application of P and others) v Secretary of State for the Home Department [2017] EWCA Civ 321

two other children. His offences were disqualified from filtering under the 'serious offences rule'. The claims also brought challenges to the 'multiple convictions rule[144]' in the case of P.

Issue

The Court considered whether the 'bright line' nature of the filtering rules, including whose which disqualifies any individual with multiple convictions, or those with convictions for offenses which appear on the serious offences list, were arbitrary or disproportionate interferences with article 8.

Decision

The Court of Appeal found that the indiscriminate nature of this rule, which allows no account to be taken of any other circumstances is "not in accordance with the law, unless there is a mechanism for independent review[145]". The Court concluded that the disclosure scheme which had been amended by the Exemptions Order following "*R (T)" was not in accordance with the law and that, in the circumstances of the case before it, the operation of the multiple conviction and serious offence rules had been disproportionate and not necessary in a democratic society*".

The appeal in W concerned a man who was convicted in the 1980s of ABH, when he was 16 years old. He received a conditional discharge. The President of the Queen's Bench Division, Sir Brian Leveson, said in his judgment: "*it is difficult to see how publication of this detail, 31 years on, is relevant to the risk of the public, or proportionate and necessary in a democratic society*.[146]"

At the time of writing, this case has been heard in the Supreme Court after the Government brought an appeal. It is awaiting judgement.

[144] See detailed information on the Filtering Rules at section 5.6.

[145] Ibid paragraph 44.

[146] Ibid paragraph 103.

See also YJLC Website "Court of Appeal finds criminal record disclosure regime unlawful" https://yjlc.uk/court-appeal-finds-criminal-record-disclosure-regime-unlawful/

The case was heard in the Supreme Court with the case of *Gallagher [2016]*[147], which concerned the filtering regime as it existed in Northern Ireland:

Facts

"In 1996 [the Claimant] *had been convicted of one count of driving without a seat belt and three counts of carrying a child under 14 in a car without a seat belt. In 1998 she was convicted of two further offences of carrying children under 14 without a seat belt*[148]*."*

Issue

The Court considered whether the multiple conviction rule which prevented the applicant's convictions form becoming 'protected' by the filtering rules, was an unjustified interference with article 8.

Decision

This case was heard in relation to the provisions of the Police Act applicable in Northern Ireland. The Court considered the question; "*Is the 1997 legislation as amended by Police Act 1997 (Criminal Record Checks: Relevant Matters) (Amendment) Order (Northern Ireland) 2014, insofar as it mandates disclosure by the State of more than one conviction indefinitely in the circumstances posited, in accordance with the law*?[149]" The Court found that the scheme under the Order failed because "*there must be a measure of legal protection against arbitrary interference with Article 8 rights.* [the Court did] *not consider that* [there were] *any or adequate safeguards with this provision which would have the effect of enabling the proportionality of the interference to be adequately examined*[150]". The Court held that there were specific failings in that there was no mechanism against indefinite retention of the records, no assessment of the risk that would be posed by non-disclosure and no assessment of the relevance of the disclosure to the position that the person has applied for, which requires a check[151].

The Court also held that the scheme failed to satisfy the test of 'necessity', justifying an infringement of a person's article 8 rights[152]. In addition, the Court held that the provisions

[147] re Gallagher's Application for Judicial review [2016] NICA 42

[148] Facts taken from Westlaw case analysis: https://login.westlaw.co.uk/maf/wluk/app/document?src=doc&linktype=ref&context=32&crumb-action=replace&docguid=I2E828A00C12011E69716D6EC90573178

[149] Ibid paragraph 67

[150] Ibid paragraph 68

[151] Ibid paragraph 70

[152] Ibid paragraphs 76 and 77

have the effect of operating "indiscriminately"[153], finding that they failed to take into account any contextualising factors such as the circumstances of the offences, age of the offender or the time lapsed since the convictions[154]. This case is also awaiting judgement from the Supreme Court.

Further, the case of *R (QSA) and others v Secretary of State for the Home Department [2018]*[155] also considered the multiple convictions rule. The claim was allowed, and a remedy granted, however it is stayed pending judgement in P, G and W from the Supreme Court.

Facts

The facts to this case are set out in section 4.2

Issue

This case considered again the multiple convictions rule, found to have been incompatible with Article 8 in R (*P).*

Decision

It was held that the Court was bound to follow that judgement even though the offences which the applicants were accused of in this case were potentially more serious. The Court held that the Government's argument that the applicants' rights were not infringed because they could choose not to apply for the job which had triggered disclosure was not correct[156].

The Claimants contended that the nature of their offending was minor and therefore it was never capable of forming a risk to the people that the disclosure regime is intending to protect. The Court rejected this argument, holding that there was nothing inherently wrong with requiring disclosure of minor offending[157].

[153] Ibid paragraph 78

[154] Ibid

[155] The Queen (on the application of QSA) and others v Secretary of State for the Home Department and another [2018] EWHC 407 (Admin)

[156] Ibid paragraph 57

[157] Ibid paragraph 69

5.2 Youth Criminal Records - The Call for Reform and Government Policy

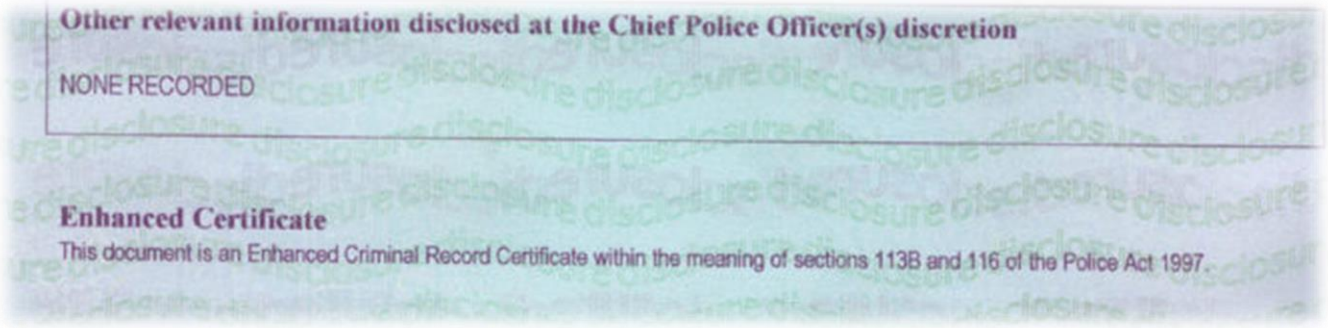
Outside of the courts there has been growing calls for reform from a range of observers, inquiries and commentators. Some of these, together with the Government's position, are set out in the table below.

The UN Committee on the Rights of the Child In 2016 the UN Committee stated that the UK should: "Ensure that children in conflict with the law are always dealt with within the juvenile justice system up to the age of 18 years, and that diversion measures do not appear in children's criminal records". (1)	*Independent Reviews* The Taylor Report stated that the system does not do enough to distinguish between adult and youth records. It recommended that spent childhood convictions and cautions should "quickly" become non-disclosable. (2) The Lammy review recommended a system of "sealing" youth records, to prevent them from being disclosable. (3)
Justice Committee Report The House of Commons Justice Committee reported on the system in 2017. They criticised the lack of flexibility in the rules (4), questioned the value of lifetime criminal records for childhood sexual offences (5) and recommends urgent reform (6). The committee stated that they believed the system fell short of the standards demanded by the United Nations Convention on the Rights of the Child (7).	*Government Position* The Government responded to the Justice Committee by stating that they believed that employers were best placed to decide how to use records once disclosed (8). The Government also maintains that they cannot take any action to reform the system until the Supreme Court gives judgement in *P and Others*, which was heard in June 2018 (9).

1. The UN Committee on the Rights of the Child: Concluding Observations on the Fifth Periodic Report of the United Kingdom of Great Britain and Northern Ireland, published in July 2016 paragraph 76(a);
2. Review of the Youth Justice System in England and Wales by Charlie Taylor. Final report. Latest version published 12 December 2016. Paragraphs 85 and 88;
3. The Lammy Review: An Independent Review into the Treatment of, and Outcomes for, Black, Asian and Minority Ethnic Individuals in the Criminal Justice System, published 8 September 2017. Recommendation 34 on page 9;
4. House of Commons Justice Committee; First Report of Session 2017–19. Disclosure of youth criminal records. Published 27 October 2017 paragraph 19;
5. As above at paragraph 20;
6. As above at paragraph 19;
7. As above at paragraphs 66-67;
8. Government Response to the Justice Committee's First Report of Session 2017 to 19: Disclosure of Youth Criminal Records. Published 31 January 2018 paragraph 49;
9. As above at paragraphs 27-30.

5.3 Enhanced certificates and "other information":

In most respects, enhanced checks are the same as standard checks.[158] However, ECRCs have a space for "other relevant information disclosed at the Chief Police Officer(s) discretion".


Other relevant information disclosed at the Chief Police Officer(s) discretion

NONE RECORDED

Enhanced Certificate

This document is an Enhanced Criminal Record Certificate within the meaning of sections 113B and 116 of the Police Act 1997.

Every ECRC will involve the DBS making enquiries with police forces that may hold information about the applicant. Those police forces will then be able to include information. This includes "non-conviction information" and is the only way in which this form of information can be included on a certificate. However, it can also include convictions and cautions that are spent and have been filtered.[159]

The issue of disclosure of non-conviction information was considered in *R (L) v Metropolitan Police [2009]*[160]*:*

> *Facts*
>
> "*The appellant obtained a job as a playground assistant. In connection with her employment, the police were required to provide her with an enhanced criminal records certificate ("ECRC"). They disclosed to the school that she had been accused of neglecting her child and non-cooperation with social services, and her employment was terminated. She claimed that the police disclosure violated her right to respect for her private life under the Human Rights Act*[161]*"*.

[158] See the introduction to this chapter at section 5.1

[159] The Quality Assurance Framework MP5. See overview guidance at page 9: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/353036/QAF_v9_OV1_Overview_of_QAF_Process_September_2014.pdf

[160] R (on the application of L) (FC) v Commissioner of Police of the Metropolis [2009] UKSC 3

[161] Summary taken from the UK Supreme Court press release: https://www.supremecourt.uk/cases/docs/uksc-2009-0104-press-summary.pdf

Issue

The Court had to consider whether the police must give weight to an individual's article 8 rights when deciding whether or not to disclose soft-intelligence.

Decision

The Supreme Court found that the 2 tests contained in s.115 Police Act (whether a record is relevant and whether it ought to be disclosed) are not inherently incompatible with article 8 rights[162]. The Court found that the disclosure of such information engaged article 8[163] because in reality any enhanced disclosure check is likely to engage article 8[164]. The Court held that in order for the disclosure regime to be compatible with article 8, there should be a presumption that, before disclosure of police information is made, an individual will get the opportunity to make representations as to why it should not be included[165]. This is now reflected in the "Statutory Disclosure Guidance" discussed at section 5.5 of this document.

The Government had suggested that the Claimant in this case could have avoided exposing private information by simply not applying for the position. However, the court found that those who apply for positions that require an ECRC **cannot be regarded as automatically consenting to their article 8 rights being violated**. The court held that when an individual consents to the disclosure of criminal records, that their consent is offered on the understanding that their article 8 rights will be respected[166].

The Court also found that the approach previously adopted by the police, that when a conflict between an individual's article 8 rights and the wider public interest exists, the public interest should prevail, was wrong. **The Court held that there should not be a presumption in either direction and that each case required consideration of the proportionality principal**[167]. This is now reflected in the Statutory Disclosure Guidance discussed at section 5.5 of this document.

However, the Court did find that specifically on the facts of the case, the disclosure was relevant to the position and the school were entitled to consider it.

[162] Ibid paragraph 47.

[163] Ibid paragraph 24

[164] Ibid paragraphs 29, 41 and 70

[165] Ibid paragraph 83 "I would have thought that, where the chief police officer is not satisfied that the applicant has had a fair opportunity to answer any allegation involved in the material concerned, where he is doubtful as to its potential relevance to the post for which the applicant has applied, or where the information is historical or vague, it would often, indeed perhaps normally, be wrong to include it in an ECRC without first giving the applicant an opportunity to say why it should not be included."

[166] Ibid paragraph 43

[167] Ibid paragraphs 44, 45, 63 and 85

In the years following this case, the number of inclusions of non-conviction information on ECRCs fell.[168]

The matter was considered again in 2018 in the case of *AR v Chief Constable of Greater Manchester Police [2018][169]:*

Facts

"In January 2011, AR was acquitted of rape by the Crown Court. He was a married man with children, of previous good character, and a qualified teacher, but was working at the time as a taxi driver. It was alleged that he had raped a woman who was a passenger in a taxi driven by him. His defence was that there had never been sexual contact with the victim. Following his acquittal, he applied for an ECRC in the course of an application for a job as a lecturer. The ECRC was issued with details of the rape charge for which he had been tried and acquitted. AR objected to this disclosure on the basis that there had been no actual conviction and it failed to give a full account of the evidence given and how the jury came to its conclusion."[170]

Issue

The Claimant in this case challenged the procedural basis on which his information had been included. He contended that it did not give context as to the evidence that resulted in his acquittal and that it was disproportionate for the information to have been included.

Judgement

The Claimant's appeal was dismissed. It was determined that the basis on which the lower court had made the assessment of proportionality, that the risk to the children with whom the Claimant hoped to work as a teacher outweighed his right to privacy, was not flawed. There was therefore no need for the appeal courts to make their own assessment.[171] The Court expressed concern at there was no guidance to employers on how to treat the disclosure of an acquittal, once disclosed, but declined to grant any relief to the Claimant.[172]

[168] In 2009/2010 there were a little more than 24,000 disclosures of non-conviction information. In 2013/2014 there were just over 9,600. See the table in the Unlock Infohub on: http://hub.unlock.org.uk/knowledgebase/local-police-information-2/

[169] R (on the application of AR) (Appellant) v Chief Constable of Greater Manchester Police and another (Respondents) [2018] UKSC 4

[170] Ibid. The Supreme Court's press summary of the case upon the handing down of judgement. https://www.supremecourt.uk/cases/docs/uksc-2016-0144-press-summary.pdf

[171] R (on the application of AR) (Appellant) v Chief Constable of Greater Manchester Police and another (Respondents) [2018] UKSC 4 paragraphs 57-65

[172] R (on the application of AR) (Appellant) v Chief Constable of Greater Manchester Police and another (Respondents) [2018] UKSC 4 paragraphs 72-76

Statutory Disclosure Guidance

There is guidance for chief police officers on when they should make disclosure of local police information, and other information they hold, called the "Statutory Disclosure Guidance"[173] ("**SDG**"). Chief officers are not entirely bound the SDG[174]. They only need to be able to show that they have had "due regard" to the SDG in coming to a decision in any given case.[175]

The Guidance contains eight principles that should be applied by chief police officers in coming to their decision. They are:

1. *There should be no presumption either in favour of or against providing a specific item or category of information.* This simply means that every piece of information should be assessed on its own merits and nothing should be automatically included or discounted because, for example, it was a record of a crime that was not pursued.

2. *Information must only be provided if the chief police officer reasonably believes it to be relevant for the prescribed purpose.* The 'prescribed purpose' is satisfied where the disclosure would be considered as a part of an application to work with children, to work in immigration advice, to operate under a taxi or certain other commercial licenses, a position relating to national security, to work with or own weapons and to work with vulnerable adults[176]. A chief police officer should reasonably believe that the information is relevant to the specific role for which the application was made[177] to include it in the disclosure. For example, it may not be appropriate for information relating to gambling offences to be disclosed, even though it relates to a prescribed purpose, if the applicant is looking to work with children.

   There are three sub-categories within this principle for a chief police officer to consider. These are that the information should be:

   a. *Sufficiently serious:* this requirement has "no hard or fast rules" to apply.[178] A chief police officer would have to consider whether or not there is sufficient gravity to the information. Information that is "trivial, or simply demonstrates poor behaviour, or relates merely to an individual's lifestyle" should not be

[173] Statutory Disclosure Guidance Second Edition, published August 2015. The Guidance was given effect by section 113B(4A) of the Police Act 1997. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/452321/6_1155_HO_LW_Stat_Dis_Guide-v3.pdf

[174] Ibid paragraph 6

[175] Ibid paragraph 6

[176] regulations 5A, 5B and 5C of the Police Act 1997 (Criminal Records) Regulations 2002 as amended

[177] Statutory Disclosure Guidance Second Edition, published August 2015 paragraph 13

[178] Ibid paragraph 15

disclosed[179]. However, less serious information may be disclosed if highly relevant to the prescribed purpose[180].

b. *Sufficiently current:* It should be less likely that older information will be disclosed. A chief police officer should also consider the applicant's age at the time of the alleged offence.

c. *Sufficiently credible:* chief police officers should consider the source of any information before disclosing it. They should consider whether there is anything in the information that makes them think it may not be true. A chief police officer should always go through the process of trying to ascertain any information that may cause them to doubt its truthfulness[181].

3. *Information should only be provided if, in the chief police officer's opinion, it ought to be included in the check:* There are two broad considerations that a chief police officer should make when applying this principle. The first is what impact disclosure will have on the applicant's private life or the private life of a third party. To do this, a chief police officer should consider whether disclosure is necessary for achieving a legitimate aim – being the prevention of crime or protection of the rights and freedoms of others or their safety. The second consideration is whether there may be a reason not to alert the applicant to the existence of police information, for example if there is an ongoing investigation that may be jeopardised if the applicant were to know about it. In these circumstances the chief police officer may take other steps such as alert the employer in confidence[182].

4. *The chief police officer should consider whether the applicant should be afforded the opportunity to make representations:* If there are questions over the truthfulness or relevance of certain information, the chief police officer should consider inviting the applicant to express their views on whether the information should be disclosed. If the chief police officer thinks that it is obvious that there is nothing the applicant can say that would change their mind on disclosure, then the applicant should not be asked to comment[183].

5. *The decision and the process of making it should be clearly recorded.*

6. *The decision should be made in a timely manner.* It is up to chief police officers to ensure that there are no unnecessary delays.

---

[179] Ibid

[180] Ibid paragraph 16

[181] "In particular, allegations should not be included without taking reasonable steps to ascertain whether they are more likely than not to be true". Ibid paragraph 18.

[182] Ibid paragraph 25

[183] Ibid paragraph 27

7. *Information for inclusion should be provided in a meaningful and consistent manner, with the reasons for disclosure clearly set out.* It should be clear to both employers and to applicants why a disclosure has been made. The wording of a disclosure should be "clear, concise and unambiguous"[184].

8. *If the chief police officer is delegating the disclosure process, that should be clearly documented.* Chief police officers should recognise the complexity of this task and take that into account when choosing a suitable officer to take on these responsibilities.

A chief police officer must also consider whether information relates to an applicant's mental health. In cases where the information tells an employer nothing about them other than their mental health, the information should not be disclosed[185].

Sexual Offences

In some circumstances applicants can apply for police information relating to a caution or conviction for sexual offences to be disregarded. If this application is successful, nothing in relation to that offence, its investigation or prosecution can be disclosed. [186] The Application Form and "Guidance Note" for applicants are annexed to this document at **Appendix 3**[187].

Quality Assurance Framework:

Chief police officers should also have regard to the Quality Assurance Framework ("**QAF**"). [188] The QAF sets out the detailed considerations that chief police officers should have in responding to an applicant's request. The QAF is assessed by the Standards and Compliance Unit ("**SCU**"); The SCU is formed as a joint working agreement between police forces and DBS staff. The SCU has the power to support good practice and to provide information and advice to police forces on compliance with the QAF. However, the SCU "will not direct the Chief Officer in respect of what disclosure decision the Chief Officer should ultimately make" and "will not interfere with individual cases"[189].

The SCU produces seven guides to chief police officers and disclosure officers regarding disclosure practices covering a range of circumstances. These are complicated and include step by step flow charts for users to follow. They are known as Method Products (MPs). The SCU also produces a set

[184] Ibid paragraph 32

[185] Ibid paragraphs 36 to 38

[186] Ibid paragraph 43. See also Protection of Freedoms Act 2012 for right to apply for SoS to disregard cautions

[187] It is published by the Home Office and can be found at:

[188] Ibid paragraph 7

[189] Overview of the Quality Assurance Framework. Published by the Disclosure and Barring Service and dated September 2014. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/353036/QAF_v9_OV1_Overview_of_QAF_Process_September_2014.pdf

of Audit Trails (ATs) which are template records to ensure appropriate notes are taken of the response to applications. A brief summary of the MPs and ATs is provided below:

Method Product	What it Covers	Summary
MP1[190]	General QAF process	A chart showing how the QAF system works. Guides the users between different MPs and ATs.
MP2[191]	Matching an applicant to information held	This template table is used to try to trace any relevant information to an applicant, and ensure that the information definitely relates to the applicant. Specifies that if the individual appears on records in the capacity of a victim, witness or officer, it should not be considered further.
MP3[192]	Relevance of locally held information.	This MP assesses the relevance of locally held police information to a request for disclosure and therefore whether it should be considered further by the chief police officer.
MP4[193]	Likelihood that someone other than the applicant will gain access to children or vulnerable people.	This MP is intended to determine whether or not, through the application, someone other than the person making the application who has been found through any search made is going to have "relevant" access to a child or third party. If they are, the MP directs the user to follow the assessment process as normal for the third party too.
MP5[194]	Filtering.	This flow chart relates to the filtering of non-court conviction records such as reprimands, cautions and warnings which are held nationally on the PNC. It is a process that directs the user to apply the Home Officer Filtering Rules if relevant. This flow allows the officer to add back in details of filtered offences.

[190] Find MP1 at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/295389/QAF_v9_MP1_QAF_Process_Map_March_2014.pdf

[191] Download MP to at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/620050/QAF_v9_AT2_December_2016.doc

[192] Find MP3 at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/634566/QAF_v9_MP3ab_Local_Info_Hit_Relevance_July_2017.pdf

[193] Find MP4 at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/274362/QAF_v9_MP4_Third_Party_Relevant_Access.pdf

[194] Find MP5 at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/634564/QAF_v9_MP5_PNC_Filtering_v2_inc_Grey_list.pdf

Method Product	What it Covers	Summary
MP6[195]	Police National Computer information.	This flow is intended to direct the user to decide whether or not information held on the PNC, which is not automatically disclosable, should be considered further for disclosure.
MP7[196]	Disclosure.	This MP contains two flows. MP7a and MP7b. MP7a is intended to guide disclosure officers to the correct decision on whether information should be disclosed once identified in the previous flows. MP7b guides the user to the best route on disclosure if it has passed all previous stages.

Audit Trail	What it Covers	Summary
AT1[197]	Systems searched for information	This AT records the locations and times of searches made for information and the "search criteria" used. The Guidance to users states that AT1 is also relevant "*where your Disclosure Unit may record specific local disclosure practices (Force Specific Policies) i.e. where your Chief Officer has risk assessed and determined that he/she would never consider disclosing certain types of information in specific circumstances*[198]".
AT2[199]	Hit Relevance Rationale	This AT records the rationale of including information that has been returned following searches. It prompts users to record the disregarding of information in certain circumstances where just a single incident has been returned. This is called a "single hit incidence", it is a quick way of removing information from consideration without going

[195] Find MP6 at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/301558/QAF_v9_MP6_PNC_Hit_Relevance_April_2014.pdf

[196] Find MPs 7a and 7b at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/295314/QAF_v9_MP7a_and_MP7b_Disclosure_Rationale_and_Method_March_2014.pdf

[197] Download AT1 at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/274381/AT1_V9_Guidance_and_Example.pdf

[198] AT1 Guidance paragraph 2.1.2. Download this document:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/274381/AT1_V9_Guidance_and_Example.pdf

[199] Download AT2 at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/620050/QAF_v9_AT2_December_2016.doc

Audit Trail	What it Covers	Summary
		through the full process (See relevant circumstances in footnote[200]). AT2 comes with a dispute resolution form[201] which enables a disclosure officer to establish the resolution to a conflict where an applicant disputes the information held about them on the PNC.
AT3[202]	Decision Rationale and Disclosure Proposal Recordings	This AT records propositions to include certain information that has not been disregarded by the processes recorded in AT2.

Sexting

The SCU has produced specific guidance for the disclosure of records made as a result of investigations into 'sexting'[203] (youth produced sexual imagery[204]). This guidance focusses mostly on a crime record that has had outcome code "Outcome 21" recorded against it, indicating that it was not considered to be in the public interest to continue with an investigation, even if that investigation might lead to a criminal charge. The QAF states that the intention of Outcome 21 is that children involved in sexting, where there are no aggravating factors, should not be criminalised. However, it notes that no

[200] AT2 provides users with the following table. They simply check a box where they consider the record to be the only example of any one of the following, and then do not consider it any further.

Offence type.	
Incident of youth produced sexual imagery (sexting) where an Outcome 21 disposal has been deemed appropriate	
Filtered Conviction/*Caution – no background information/M.O. held by force	
Filtered Conviction/*Caution - background information/M.O. held by force shows record is not relevant	
Drink related – no violence.	
Caution (including those not recorded on PNC) over 5 years old, with **no element of harm to children or vulnerable adults and not considered relevant.	
Arrested, released no further action, where the reason for arrest was **not** connected with sex, violence, threat of violence, drugs, firearms, offensive weapon, or mental health.	
Charged with (but not convicted) or suspected of an offence of theft more than 5 years ago.	
Charged with (but not convicted) or suspected of an offence of minor assault (S47 or less) more than 5 years ago, that did **not** involve a child under 18 years of age or a vulnerable adult.	
Possession of a controlled drug for personal use.	

[201] Download the dispute resolution form here:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/616996/AT12_Dispute_Form_May_2017.doc

[202] Download AT3 at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/654631/QAF_v9_AT3_October_2017.pdf

[203] GD8–Youth Produced Sexual Imagery-Guidance for Disclosure.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/578979/GD8_-_Sexting_Guidance.pdf

[204] There is no universally accepted definition of sexting, but this one is used by the College of Policing in their briefing note on Sexting and Outcome 21 and is therefore the most relevant definition here.

guarantee should have been given that the information will not be disclosed as it is up to each individual police chief. It provides no further clarity or reassurance[205].

To reduce the chance of an Outcome 21 recording being disclosed, the QAF provides that a disclosure officer should use 'AT2', an audit trail (described in the table above) that enables the user to discount information from disclosure, in certain circumstances, without having to go through the full assessment process. One of these circumstances is when there is a single "outcome 21" recording. However, where there is more than one Outcome 21 record, or any other record in addition to the Outcome 21, then the disclosure officer cannot use AT2 and must go through the full process outlined in the Disclosure Guidance and the Method Products outlined above in section 5.5 and 26[206]. This means that there will be "no presumption" either for or against disclosure where AT2 does not apply.

Outcome 21, a relatively new outcome developed specifically for youth produced sexual imagery, is the only such outcome code to come with specific guidance relating to disclosure. Any other outcome code, including those recorded for sexual imagery prior to the creation of Outcome 21 in 2016, must go through the full disclosure consideration process.

There is currently no clarity on how consistently Outcome 21 is applied, or how effective it is at reducing the chances of disclosure (Just for Kids Law are, at the time of writing, undertaking research through Freedom of Information requests and will update this guidance with our findings).

Challenging a decision by the police to include information on an enhanced certificate

If further information is included on an ECRC about an individual, there are mechanisms available to have that decision reviewed. Initially, disputes are resolved through the disclosing police force.[207] Applicants should use "Certificate Dispute Form (AF15(a))".[208]

The police should use AT12 of the Quality Assurance Framework to resolve disputes, but this does not give officers any specific direction on the process of considering the applicant's petition. AT12 instead asks that officers accept, accept in part or reject a dispute and record their rational for doing so.

There is no limit or specified grounds on which an applicant can raise an objection, but the Quality Assurance Framework suggests that common grounds might be that:

- In relation to non-conviction information:
    - disclosed information is not about them;
    - disclosed information contains factual inaccuracies;

[205] Ibid pages 2 and 3

[206] ibid

[207] Police Forces are directed to utilise Audit Trail 12 to record their consideration of an applicant's dispute. See QAF guidance on completing AT12 at: https://www.gov.uk/government/publications/quality-assurance-framework-version-nine-qaf-v9

[208] This form can be downloaded at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/425342/DBS_certificate_dispute_form_v0.1.docx

- disclosed information is not relevant, complete, balanced or fair;
- the reasons given for disclosure are unreasonable; and

- in relation to conviction information:
  - applicant believes that the entire PNC record does not belong to them;
  - an individual conviction/caution etc. within a record does not belong to them;
  - an incorrect/incomplete sentence has been recorded;
  - the conviction/caution differs from that which the applicant believes they have.

If a dispute is not resolved through this internal procedure then an applicant can escalate it to the "independent monitor", a functionary of the DBS.[209] This route is only open to applicants in the event that they believe that the included non-conviction information is:

- not relevant to the position applied for; or
- should not be included in the certificate.[210]

There are no agreed or mandatory turnaround times for either of these dispute procedures. However, a dispute must be raised within 3 months of the date of the DBS Certificate.[211]

Complaints can also be raised with the Information Commissioners' Office (**"ICO"**). The ICO will consider whether or not the data handler has breached the Data Protection Act, the Freedom of Information Act and its own guidance and can take enforcement action if it finds unsatisfactory conduct.[212] The ICO issues a relevant guidance titled the Data Sharing Code of Practice.[213] However, at the time of writing this has not been updated to reflect the changes to the law brought in by the Data Protection Act 2018. The ICO is therefore not discussed further.

If these avenues are exhausted or not appropriate, then a claim for Judicial Review will be the last method of recourse.

Unlawful or fraudulent applications to the DBS

Under Part V Police Act 1997 there are a number of offences that relate to the obtaining, creating and amending criminal records certificates. Among them, an offence is committed when:

[209] https://www.gov.uk/report-problem-criminal-record-certificate/appeal-against-a-mistake

[210] Ibid

[211] Ibid

[212] ICO published guidance titled "How we Deal with Complaints and Concerns: a guide for data controllers".

[213] This can be found at: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

> *"*[a person] *knowingly makes a false statement for the purpose of obtaining, or enabling another person to obtain, a certificate under this Part[214]".*

Individuals therefore commit an offence if they make an application for a DBS certificate about their own records under false pretences, for example by claiming that they are applying for a position that is exempted from the ROA.

However, additionally, it is an offence for registered bodies to make requests for standard and enhanced certificates when they are *not* entitled to ask an exempted question.

> It has been reported that some organisations make checks as a blanket rule, including when they are not actually entitled to ask an exempted question. This issue has been discussed by Unlock, a leading NGO with expertise in assisting people with convictions and criminal records. Unfortunately, they have found that enforcement action against bodies that do this is non-existent. Regardless, they recommend that anyone who comes across such activity make a report to the Ministry of Justice, who own the ROA.
>
> (http://www.the-record.org.uk/unlock-people-with-convictions/unnecessary-checks-are-a-crime-and-should-be-reported-to-the-police/.)

5.4 Sharing of Police Information Under Other Police Powers

MoPI obliges the Police to, "*give access to police information in response to a request from any person or body to the extent that the chief police officer believes this request to lawful and reasonable for the purposes of* [the regulations] *and in compliance with guidance issued under this Code[215]*". (Note: when MoPI says "the guidance issued under this Code", this refers to the Authorised Professional Practice Guides issued by the College of Policing".)

The police have several powers to share information.

Common law powers

The APP describes the test as to whether Chief Police Officers can share information under their common law powers. They can only do this where there is a "pressing social need".[216]

The National Police Chiefs' Council has provided guidance to the police on using these common law powers.[217] This guidance describes a pressing social need as including "*the safeguarding, or protection*

[214] Police Act 1997 s123(2)

[215] Code of Practice on the Management of Police Information July 2005 paragraph 4.8.4

[216] APP on Information Sharing: https://www.app.college.police.uk/app-content/information-management/sharing-police-information/#common-law

[217] The guidance is titled "Common Law Police Disclosures (CLPD) – Provisions to supersede the Notifiable Occupations Scheme (NOS)". It can be found at: https://www.app.college.police.uk/wp-content/uploads/2016/08/NPCC-2017-Common-Law-Police-Disclosures-CLPD-—-Provisions-to-supersede-the-Notifiable-Occupations-Scheme-NOS.pdf

from harm, of an individual, a group of individuals, or society at large".[218] It then goes on to direct that it will normally be arrests or information extracted through interview that would lead the police to invoke these powers. It directs that the police will not be empowered to make disclosure of convictions as there will not be an urgent need due to the lapse of time from which the Police became aware of the information, and the fact that processes already exist for employers to obtain information concerning convictions.[219]

Statutory powers

The police possess Statutory Powers under the Data Protection Act, Freedom of Information Act, Safeguarding Vulnerable Groups Act, and the Police Act to share information[220]. In exercise of these powers the Police may set up information sharing agreements with other bodies. These are not discussed further in this guide.

[218] Ibid

[219] Ibid

[220] Authorised Professional Practice guide on Information sharing: https://www.app.college.police.uk/app-content/information-management/sharing-police-information/#statutory-obligation

6. Disclosure by Police Certificate

This section covers:

1. *The process of obtaining a certificate evidencing one's criminal history when looking to emigrate or obtain a visa for foreign travel to certain countries:* to work and travel abroad, it is not necessary or possible to obtain a certificate from the DBS. For travel to, and work within, some countries a Police Certificate is required.

2. *The 'stepped down' model of filtering records from such certificates:* what is included on these certificates differs from those issued by the DBS. The model that is followed is called the stepped down model, and it can lead to the filtering of convictions and cautions that would not be filtered on a DBS certificate.

6.1 Introduction to police certificates

ACRO Criminal Records Office, a national policing body that provides some services to "law enforcement and public protection teams"[221], issues "Police Certificates to people who want to emigrate to, or obtain a visa for, foreign countries. A certificate can be obtained for such travel to any country[222]. ACRO list the following countries as being among those requiring a certificate: Australia, Belgium, Canada, Cayman Islands, New Zealand, South Africa and the United States of America"[223].

Applications for a police certificate are made directly to ACRO.[224]

The step-down model

Certificates will display convictions and cautions, subject to the "step-down" model.[225] The step-down model takes records out of the possibility of disclosure after specified periods of time have elapsed. The time taken for the record to step down depends on the offence, the sentence or other disposal, the age of the applicant at the time of the record's creation and whether or not other offences are committed during the "clear period". The clear period is the length of time taken between the record's creation and the time which it is stepped down.

Categories of offence

The amount of time taken for convictions and cautions to be stepped-down is dependent on the type of offense. Offences are split into categories A, B and C. Category A includes offences deemed to be

[221] ACRO website "about us". https://www.acro.police.uk/About_Us.aspx

[222] ACRO Police Certificates Frequently Asked Questions webpage: https://www.acro.police.uk/Police_Certificates_FAQs.aspx#Countries_for_which_a_Police_Certificate_is_required

[223] Ibid

[224] ACRO website "Police Certificates" section. https://www.acro.police.uk/police_certificates.aspx

[225] ACRO Criminal Records Office guidance titled: "Step-Down Model" dated 5 January 2018. https://www.acro.police.uk/uploadedFiles/Content/ACRO/STEP%20DOWN%20MODEL%20v2.1.pdf

the most serious and C the least. The only way to know which category an offence falls into is by reference to exhaustive lists published by ACRO in its guidance.[226]

Length of clear period

The table below shows the time taken for different categories of offence to be stepped-down dependent on the age of the applicant at the time of the offense and the result of the alleged offending.[227] Records of category A offences that resulted in a custodial sentence will never be stepped down.[228]

PERSON	OUTCOME	SENTENCE	OFFENCE	STEP DOWN NON-POLICE USERS
ADULT	CUSTODY	6 MONTHS OR MORE	A B C	N/A 35 YEARS 30 YEARS
YOUNG PERSON	CUSTODY	6 MONTHS OR MORE	A B C	N/A 30 YEARS 25 YEARS
ADULT	CUSTODY	LESS THAN 6 MONTHS	A B C	N/A 20 YEARS 15 YEARS
YOUNG PERSON	CUSTODY	LESS THAN 6 MONTHS	A B C	N/A 15 YEARS 10 YEARS
ADULT	NON-CUSTODY		A B C	20 YEARS 15 YEARS 12 YEARS
YOUNG PERSON	NON-CUSTODY		A B C	15 YEARS 12 YEARS 10 YEARS
ADULT	CAUTION		A B C	10 YEARS 5 YEARS 5 YEARS

[226] Ibid, see tables in Appendix 2 starting on page 12.

[227] Table is copied from the ACRO guidance Appendix 1 on page 11

[228] Ibid paragraph 3.1

PERSON	OUTCOME	SENTENCE	OFFENCE	STEP DOWN NON-POLICE USERS
YOUNG PERSON	REPRIMAND OR WARNING		A B C	10 YEARS 5 YEARS 5 YEARS
ADULT OR YOUNG PERSON	PND, ACQUITTAL, ARREST, DECRIMINALISED, OTHER (Lie on File, Sine Die etc)		A B C	ON RESULT BEING ENTERED ONTO RECORD[229]
ADULT OR YOUNG PERSON	IMPENDING PROSECUTION, UNDER INVESTIGATION		A B C	STEPDOWN APPLIED WHEN OUTCOME KNOWN

Contents of a police certificate record

A certificate will include personal details and passport information together with any PNC records which are not stepped down in accordance with the clear periods detailed above. No further elements of a person's police records are included.[230]

[229] This phrasing is not the original text as the original text appears incomplete. This text has been updated with information from paragraph 3.26 of the guidance.

[230] See the ACRO Frequently Asked Questions which states that what is included is "convictions" in accordance with he step down model outlined in the guidance. This is misleading in the sense that the guidance makes clear that pending investigations and other records can be included.

7. Disclosure (self)

This section covers:

1. *The obligations that exist on an individual to disclose information about their criminal record:* individuals who apply for employment and certain courses of education or training may be obliged to disclose spent and unspent convictions.

2. *The power to deny the existence of spent convictions in certain circumstances:* the Rehabilitation of Offenders Act empowers people to deny that they have a criminal record at all when their convictions are spent, and the employer is not asking a question which is exempt under the Act's Exemptions Order.

7.1 Introduction to the requirement to make self-disclosure

Self-disclosure is the process through which an individual is expected to volunteer details of their criminal record.

The information that an employer is entitled to expect an applicant or employee to disclose is, in most circumstances, the same as that which the employer would receive on a certificate issued by the DBS for the same position.

An employer cannot require an applicant to self-disclose information about spent convictions unless applying for a job listed in the schedules to the Rehabilitation of Offenders Act (Exemptions) Order[231]. If it is not included in one of these schedules, applicants are allowed to deny the existence of any spent convictions[232]. If, in these circumstances, an employer refuses an application for employment or later dismisses the employee on the basis of their denial of the conviction's existence, or because they have spent convictions, the individual may be able to bring a claim to an employment tribunal.

Applicants may be asked to disclose unspent convictions. An applicant could be held to be dishonest if they failed to do so[233].

[231] Unlock infohub guidance to individuals titled: Legally, Need to Disclose? http://hub.unlock.org.uk/knowledgebase/need-disclose/

A list of these occupations is in the introduction to Criminal Records Checks at section 5.1

[232] Ibid

See also explanation of spent convictions in the introductory chapter.

[233] Ibid

Guidance from Weightmans Solicitors entitled "Employees with criminal convictions: A right to work?" https://www.weightmans.com/insights/employees-with-criminal-convictions-a-right-to-work/

When is an applicant protected from self-disclosure?

Rehabilitation of Offenders Act 1974

The Rehabilitation of Offenders Act (ROA) provides that when a conviction becomes 'spent' the data subject is not required to disclose it even if asked to do so. Requests to volunteer information about convictions which are spent can be answered as if the offence in question had never been committed[234], unless the applicant is being asked an 'exempted question'.

Rehabilitation of Offenders Act 1974 (Exemptions) Order 1975 ("the Order")

Section 3(1) of the Order explains that, when an applicant is asked to disclose spent convictions in relation to a job listed in the Order's schedules, the protections of the ROA do not apply. Therefore, applicants applying for such positions are not able to deny the existence of spent convictions and receive no protection against dismissal if they fail to do so.

Filtering

Employers and educators are not allowed to use protected convictions, even if they become aware of them. They therefore should not ask for disclosure of protected convictions and cautions.[235]

Disclosing convictions

Taken together, this means that applicants can only decline to self-disclose spent conviction when the employer, or other organisation requesting information, is not *lawfully* asking an exempted question. If a data-subject is lawfully asked an exempted question they must disclose all convictions, including those that are spent, but not those that are filtered under the Home Office Filtering Rules.

The case of *HA v University of Wolverhampton*[236] considered a university's right to access spent convictions.

> *Facts*
>
> The Claimant in this case was a student enrolled on a pharmaceuticals course at the University of Wolverhampton. In his youth he had been convicted of assault following a fight in a school yard and then of robbery when, as part of a group, he had stolen from another young person in a park. He did not disclose these to University of Wolverhampton when asked. The Claimant claimed that he did not disclose following advice from his probation officer who had explained that he did not have to do so.
>
> When the university found out about the convictions they expelled the Claimant. He brought a claim to the High Court, claiming that the university was not entitled to ask an exempted question under the Exemptions Order and, therefore, the Claimant was not obliged to disclose his convictions as they had become spent.

[234] See explanation of spent convictions in the introductory chapter.

[235]

[236] HA v University of Wolverhampton & Ors (Rev 1) [2018] EWHC 144 (Admin)

Issue

The Court considered whether the University had a right to access the Claimant's offending history, and whether he should have been expected to volunteer it.

Decision

The Court found that:

1. as pharmaceuticals is a profession listed in the Exemptions Order, and as the university acted as a gatekeeper for that profession, it was entitled to ask an exempted question;

2. because the course involved practical experience which may include contact with vulnerable adults, the University was entitled to ask an exempted question; and

3. the Claimant was obliged to disclose the convictions (the exclusion however was quashed on grounds relating to the procedure through which it was administered).

A note on case law: Many of the challenges to the disclosure regime (set out above) are also relevant for self-disclosure. For example, the case of P v SoSHD, which challenged the bright lines rules in the Home Office Filtering Rules is applicable to self-disclosing convictions too.

8. Use

This section covers:

1. *How employers and other bodies can make decisions based on the disclosure of criminal records:* private employers and providers of education or training can make decisions regard for the DBS's guidance to registered bodies, although oversight of this procedure is poor. If they were not lawfully entitled to obtain the disclosure they received, it cannot be considered at all. For example, an employer that was not entitled to ask an exempted question would be acting unlawfully to dismiss someone based on disclosure of that conviction.

2. *How information on police systems can be shared with other agencies:* agencies other than the police may have access to the PNC and the PND, and all police forces do. Information can be accessed and shared often very easily, without making a request to the initial data controller. MoPI sets out some of the principals to apply to this practice.

8.1 Introduction to the Use of Criminal Records

Police records can be used in a variety of ways. Perhaps most common is the assessment of disclosed information by employers and education providers, as part of an application for employment or a voluntary position. Information can also be shared between the police and other agencies and can be used in future prosecutions and investigations.

8.2 Use of information by employers

The requirement not to consider spent or protected convictions

Spent convictions

Spent convictions cannot be considered by an employer for a position to which the Rehabilitation of Offenders Act applies.[237] In addition, they cannot be lawfully used as grounds for a person's dismissal.

It has been covered in the section of this guide "Disclosure (self)", that where the Rehabilitation of Offenders Act applies there is no obligation to volunteer information about spent convictions. A person cannot be dismissed for acting dishonestly if they do this and the convictions subsequently come to the employer's attention.

Protected convictions

The Home Office Filtering Rules, discussed in this guide at section 5.1, prevent employers from considering convictions that are "protected" under the filtering rules, if disclosed.[238]

[237] Rehabilitation of Offenders Act s4(3)(b): "a conviction which has become spent or any circumstances ancillary thereto, or any failure to disclose a spent conviction or any such circumstances, shall not be a proper ground for dismissing or excluding a person from any office, profession, occupation or employment, or for prejudicing him in any way in any occupation or employment."

[238] The DBS Filtering Guide published on the Government website: https://www.gov.uk/government/publications/dbs-filtering-guidance/dbs-filtering-guide

The case of *R (R) v NPCC and others [2017]*[239] considered the issue of police use of information that was protected.

Facts

The case involved an individual applying to become a police support officer, with a view to becoming a police constable. The police accessed a caution she had been issued when younger, by viewing it through their direct access to police databases.

Issues

The Court considered whether they were entitled to use the information, because they had not been entitled to have access to it, as it was protected under the filtering rules.

Decision

The court held that, the police did not have the right to request the information which the Claimant disclosed. The court therefore held that it was unlawful for the police to consider it as a part of their decision-making process.[240]

The requirement to take a "fair" approach to considering criminal records

The Guidance on the Rehabilitation of Offenders Act 1974 ("**GoROA**") provides guidance to employers on how to 'use' information that is disclosed to them. The guidance does not bind employers, instead stating that "*each employer is best placed to consider whether a person's convictions (either before they have become spent, or, in the case of activities listed on the Exceptions Order, when they are spent) make him or her unsuitable for a particular job*". It encourages employers to reach a balanced decision, having regard to:

a. the person's age at the time of the offence;
b. how long ago the offence took place;
c. whether it was an isolated offence or part of a pattern of offending;
d. the nature of the offence;
e. its relevance to the post or position in question; and
f. what else is known about the person's conduct before and after the offence.

The Revised Code of Practice for Disclosure and Barring Service Registered Persons requires that employers don't "discriminate automatically" on the basis of past convictions or cautions and requires employers to have a "fair and clear" policy in place with regard to hiring ex-offenders. This Code of

[239] The Queen (on the application of "R") v The National Police Chief's Council [2017] EWHC 2586 (Admin) 2017 WL 04652934

[240] Ibid Paragraph 77

Practice is a statutory instrument and breach of this code can, in law, result in a body's registration with the DBS being suspended.[241]

The case of *HA v University of Wolverhampton*[242] discusses the correct application of a body's established policy when using records.

Facts

The facts of this case are set out at section 6.3 above.

Issues

In relation to 'use', the court considered whether the University were entitled to expel the Claimant on the strength of the police records which were disclosed to them.

Decision

The Court found that the use of the information was unlawful. The Court held that the disciplinary panel that excluded him failed to follow its own procedure[243] and failed to take mitigating circumstances to the convictions into account. (This decision was made on a purely procedural basis, the court stressed that once the correct procedural steps had been followed, it may still be correct to proceed with the exclusion[244]).

The case of *R (R) v NPCC and others [2017*][245] considered what weight an employer should ascribe to disclosed information about an applicant.

Issue

The Court considered whether the use of records was a sufficient safeguard against infringements of Article 8. The Defendant argued that a person's article 8 rights were protected from unjust interferences through disclosure, because organisations will respect article 8 when using those records. Essentially, that there is "regulation through use" which protects an individual's article 8 rights.

Decision

The High Court in this case explained the issue of 'use' as distinct from 'disclosure' by highlighting that "[the Claimant] *was rejected at a very early stage of the recruitment process,*

[241] Revised Code of Practice for Disclosure and Barring Service Registered Persons dated November 2015 page 4. Section titled "what happens if this code is breached?"
[242] HA v University of Wolverhampton & Ors (Rev 1) [2018] EWHC 144 (Admin)

[243] Ibid paragraphs 159-173

[244] Ibid paragraph 174

[245] The Queen (on the application of "R") v The National Police Chief's Council [2017] EWHC 2586 (Admin) 2017 WL 04652934

purely on the strength of [a] *reprimand*". The Claimant had applied to become a police support officer with the ambition of becoming a police constable. The Court summarised the response to her application as "*deliberately off-putting*" because they had purposely written their response to give the impression that "*the chances of her ever being appointed as an officer are slim, and in reality, non-existent*[246]".

The Court found that this had been a "laboratory experiment" of the concept of regulation through use that had shown that "*regulation through use has conspicuously failed.*" Explaining that; *"the present case provides powerful support for the Claimant's broader argument that there is an inherent risk in a rule which focuses only upon use. Since the 2013 amendments the Police force has not proven able to introduce a policy which is consistent with the changes to the law. Nor have they been able to draft guidance which takes account of Article 8*."

Code of Practice on the Management of Police Information

They principals of MoPI relevant to the use of police information are[247]:

- Sharing of police information within the UK police service;
- Information held, subject to guidance in the APP, should be made available to other police forces for a 'police purpose';
- Chief police officers should arrange for the sharing of information either in response to requests for information or by holding it on IT systems which other forces have access to;
- This last provision may be made effective by the Police National Computer and the Police National Database.

Lack of Enforcement and Oversight

It is unclear how regularly organisations lose their registration with the DBS because of non-compliance. An independent report by the National Audit Office expressed concern that "*there are no checks on how employers use information provided by the DBS".*[248] This lack of oversight was highlighted as a concern by the Supreme Court in July 2018 in the case of *AR v Greater Manchester Police*.[249]

[246] Ibid paragraph 74

[247] Ibid paragraph 4.1

[248] National Audit Office report: Investigation into the Disclosure and Barring Service. Dated 1 February 2018: https://www.nao.org.uk/wp-content/uploads/2018/02/Investigation-into-the-Disclosure-and-Barring-Service.pdf

[249] R (on the application of AR) (Appellant) v Chief Constable of Greater Manchester Police and another (Respondents) [2018] UKSC 47 Paragraphs 75 and 76.

Further Reading:

1. Authorised Professional Practice, Management of police information: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/
2. Briefing Note: Police action in response to youth produced sexual imagery ("Sexting"). Version 1.0: http://www.college.police.uk/News/College-news/Documents/Police_action_in_response_to_sexting_-_briefing_(003).pdf
3. Code of Practice on the Management of Police Information: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf
4. Deletion of Records from National Police Systems: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/430095/Record_Deletion_Process.pdf
5. Government Response to the House of Commons Justice Committee's Report on the Disclosure of Youth Criminal Records: https://www.parliament.uk/documents/commons-committees/Justice/JC-criminal-records-response.pdf
6. Growing Up, Moving On: the International Treatment of Childhood Criminal Records. Produced by the Standing Committee for Youth Justice. 2016 full version: http://scyj.org.uk/wp-content/uploads/2016/04/ICRFINAL.pdf. 2017 summary with policy recommendations: http://scyj.org.uk/wp-content/uploads/2016/04/Growing-up-moving-on-Executive-Summary.pdf
7. Home Office Counting Rules. Crime Recording General Rules: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/694432/count-general-apr-2018.pdf
8. Home Office Statutory Disclosure Guidance Second Edition: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/452321/6_1155_HO_LW_Stat_Dis_Guide-v3.pdf
9. House of Commons Justice Committee Report: Disclosure of Youth Criminal Records: https://publications.parliament.uk/pa/cm201719/cmselect/cmjust/416/416.pdf
10. The Lammy Review, Chapter 6 "Rehabilitation": https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643001/lammy-review-final-report.pdf
11. Review of the Youth Justice System in England and Wales by Charlie Taylor. Paragraphs 82-89: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/577103/youth-justice-review-final-report.pdf

Appendix 1: Home Office Counting Rules Annex B. List of Serious Offences in schools.

Serious incidents referred to within the 'Crime Recording by Police Officers Working in Schools' guidance are defined as:

a) All Indictable Only offences.
(b) All offences within HOCR classifications;

a. 5D (Assault with Intent to Cause Serious Harm),
b. 10B (Possession of Firearms),
c. 10C (Possession of other Weapons),
d. 10D (Possession of Article with Blade or Point).
e. 11A (Cruelty to Children),
f. 13 (Child Abduction),
g. 23 (Incest),
h. 36 (Kidnapping),
i. 70 (Sexual Activity with a Person with a Mental Disorder),
j. 71 (Abuse of Children through Prostitution/Pornography),
k. 86 (Obscene Publications),
l. 88A (Sexual Grooming),
m. 92A (Trafficking in Controlled Drugs),
n. 92D (Possession of Controlled Drugs),
o. 92E (Possession of Cannabis),
p. 106 (Modern Slavery),

(c)
All sexual assaults.
Any other offence is serious only if its commission has led to any of the consequences set out below, or is intended to lead to any of those consequences:

(a) serious harm to the security of the State or to public order;
(b) serious interference with the administration of justice or with the investigation of offences or of a particular offence;
(c) the death of any person;
(d) serious injury to any person;
(e) substantial financial gain to any person; and
(f) serious financial loss to any person.

If any other offence consists of making a threat, it is 'serious' if the consequences of carrying out the threat would be likely to lead to one of the consequences set out above at (a) to (f).
The term 'injury' includes any disease and any impairment of a person's physical or mental condition.

Financial loss is 'serious' for the purpose of the section if, having regard to all the circumstances, it is serious for the person who suffers it. Whether or not a loss, actual or intended, is serious will depend partly on the victim's circumstances.

Appendix 2: National Retention Assessment Criteria template

National Retention Assessment Criteria Template

For advice on completing this form, see APP on information management

Record		Date of review	
Review type (triggered or scheduled)		If review was triggered explain how/why	

Retention criteria

Factors – risk or harm	Yes/No	If 'Yes' provide an explanation of how/why
1 Is there evidence of a capacity to inflict serious harm, eg, threats, violence towards partner, hate-based behaviour, predatory behaviour?	☐ Yes ☐ No	
2 Are there any concerns in relation to children or vulnerable adults?	☐ Yes ☐ No	
3 Did the behaviour involve a breach of trust?	☐ Yes ☐ No	
4 Is there evidence of established links or associations which might increase the risk of harm, eg, gang membership, contact with known paedophiles or other established criminal groups?	☐ Yes ☐ No	
5 Is there evidence of substance misuse?	☐ Yes ☐ No	
6 Are there concerns about the individual's mental state, eg, symptoms of mental illness, obsessive or compulsive behaviour, morbid jealousy, paranoia, lack of self-control?	☐ Yes ☐ No	
7 Any other reasons?	☐ Yes ☐ No	

Is the information under review proportionate and still necessary for a policing purpose?	☐ Yes	☐ No
Is the information under review adequate and up to date?	☐ Yes	☐ No

Outcome of review			
Completed by		Authorised by	

Appendix 3: Disregarding Certain Criminal Convictions Chapter 4

Disregarding Certain Criminal Convictions

Chapter 4 Part 5 Protection of Freedoms Act 2012

Application Form &
Guidance Notes for Applicants

Home Office

Part 5 Protection of Freedoms Act 2012. Application Form &Guidance Notes for Applicants

GUIDANCE FOR APPLICANTS

This application form is for use by anyone seeking to make an application to the Secretary of State for the Home Department ("Home Secretary") to have one or more of their convictions for offences, as listed in Chapter 4, Part 5 of the Protection of Freedoms Act 2012, formally disregarded.

The word "conviction" includes a conviction, caution, warning or reprimand unless otherwise specified.

AM I ELIGIBLE TO APPLY TO HAVE MY CONVICTION DISREGARDED?

You may only apply to have **your** conviction(s) disregarded. Applications made on behalf of a third party will not be accepted. Where you ask someone to help you to complete the application form, you must still sign to confirm that the details contained therein are accurate and complete to the best of your knowledge.

Convictions under the following provisions may be eligible to be disregarded:

- Section 12 of the Sexual Offences Act 1956
- Section 13 of the Sexual Offences Act 1956
- Section 61 of the Offences against the Person Act 1861
- Section 11 of the Criminal Law Amendment Act 1885

In addition, convictions under the following provisions (in respect of acts contrary to the provisions listed above) may also be eligible to be disregarded:

- Section 4 of the Vagrancy Act 1824
- Section 45 of the Naval Discipline Act 1866
- Section 41 of the Army Act 1881
- Section 41 of the Air Force Act 1917
- Section 70 of the Army Act 1955
- Section 70 of the Air Force Act 1955
- Section 42 of the Naval Discipline Act 1957

Applications relating to any other convictions will **not** be accepted.

In order for an eligible conviction to be disregarded it must appear to the Home Secretary that (a) all parties involved in the conduct constituting the offence consented to it and were aged 16 or over at the time the offence was committed, and (b) any such conduct now would not be an offence under section 71 of the Sexual Offences Act 2003.

i

COMPLETING THE APPLICATION FORM:

There are two sections to the application form:

Section A relates to your current personal details and **must** be completed in full in order for an application to be accepted. You only need to complete section A once per application, regardless of the number of convictions you are applying to have disregarded. Failure to provide the information requested in section A will result in your application being rejected.

Section B relates to your personal details at the time the offence was committed and the details of the offence itself. This section should be completed as fully as possible. If you are applying to have more than one conviction disregarded, please copy section B as many times as necessary and complete a separate section B for each conviction. This includes where you were convicted on the same occasion for more than one offence. The more information you provide, the easier it will be to locate relevant records and progress your application quickly.

The application form includes further guidance on how to complete each section. When complete, you should sign and date the application form at the bottom of section A and at the bottom of each section B completed. Please ensure that you have included copies of any materials or documents that you wish to submit in support of your application, along with evidence of your identity and current address, and return it to:

Chapter 4 Applications, SPPU, 4th Floor Fry Building, 2 Marsham Street, London, SW1P 4DF
Or by e-mail to **chapter4applications@homeoffice.gsi.gov.uk**

CONFIRMING YOUR IDENTITY AND ADDRESS:

Criminal record information is sensitive personal information and its management is strictly governed. In order to safeguard the information and ensure that it is only disclosed to the person that it relates to, and processed only as far as necessary to progress your application, we require you to provide **copies** of two documents to confirm (a) your identity, and (b) your current address. Please **do not** send original documents as we are unable to return them to you. Further guidance on which documents are acceptable as evidence of your identity and address can be found in section A of the application form.

PROTECTING YOUR PERSONAL INFORMATION:

All information that you provide will be treated in the strictest confidence. We will never disclose the information to any person or organisation not involved in the process without your express consent to do so. If you would like us to contact someone else acting on your behalf in respect of this application, you should enclose a signed letter along with your application setting out the contact details of the person acting on your behalf and stating that you consent to us discussing your application with that individual / organisation.

We will retain details of your application for a period of 6 years to enable us to deal with any subsequent queries or legal challenges that may arise. It will not be accessed for any other purposes and all personal details will be deleted after this period.

It is **strongly recommended** that you keep all the official correspondence you receive in relation to this application, as a record of what has happened. Please note that it will not be possible to provide further copies of correspondence after your application has been completed and your personal details deleted.

WHAT HAPPENS NEXT?

On receipt of your completed application relevant details will be processed. If the matters raised in your application are not eligible to be disregarded you will receive a letter to that effect. In all other cases you will receive an acknowledgement that your application has been received and is being processed.

In order to process your application, the Home Office will contact all relevant data controllers (the Police, HM Courts & Tribunals Service and, if relevant, the Armed Forces Service Police) and request them to review their records and provide copies of any relevant documents to the Home Secretary to enable a decision to be made. Where an application raises complex issues, or where the available evidence is unclear or contradictory, it may be passed to an independent advisory panel which will consider the application carefully and make recommendations to the Home Secretary.

Once the Home Secretary has made a decision, you will be informed of the outcome. If your application is successful, the Home Secretary will write to the relevant data controllers and require them to delete or annotate their records accordingly. Each data controller will write to you to confirm that this has been done.

EFFECT OF DISREGARD:

Once the Home Secretary has given notice that a conviction has been disregarded and a period of 14 days thereafter has elapsed, a successful applicant will be treated in all circumstances as though the offence had never occurred and need not disclose it for any purpose. Official records relating to the conviction that are held by prescribed organisations will be deleted or, where appropriate, annotated to this effect as soon as possible thereafter.

WHAT IF I DISAGREE WITH THE HOME SECRETARY'S DECISION?

If you disagree with the decision reached by the Home Secretary and either have further evidence to submit or consider that an error was made on your initial application form, you should contact the Home Office so that your application can be reviewed. If you consider that the final decision reached in relation to your application is wrong, you have the right under the provisions of the Protection of Freedoms Act 2012 to seek leave to appeal the decision to the High Court.

This page has been deliberately left blank

Section A: Personal details

Your current personal details:

Forename(s): .....

Surname: .....

Date of Birth: .....

Place of Birth: .....

You must confirm your identity by enclosing a copy of one of the identity credentials listed in the guidance notes.

Your current address:

Property No. / name: .....

Street / Road: .....

Town / City: .....

County: .....

Postcode: .....

You must confirm your address by enclosing a copy of one of the verification documents listed in the guidance notes opposite.

Your preferred method of communication:

☐ Post (as address above)

☐ Post (alternative address - please state below)

.....

.....

.....

.....

.....

☐ Email (please state e-mail address below)

.....

How many convictions are you applying to have disregarded? ☐

Declaration:

I confirm that the information I have provided is correct to the best of my knowledge. I understand that the information I have provided may be stored and shared with other relevant organisations, and prescribed records searched, only as far as necessary to process my application.

Current personal details:

Enter your current details. If your name has changed since you were convicted, enter your former name in section B.

We need to confirm your identity before accessing your records. Please enclose a copy of one of the following documents:

- Passport (biographical data page)

- Driving licence (photo card and / or paper counterpart)

- HM Forces ID card

- Firearms licence

- Birth / Adoption certificate

Current address details:

Enter your current address details, including your postcode.

To confirm your address, please enclose a recent copy of one of the following documents:

- Bank / Building Society statement

- Utility bill

- Credit / store card statement

- Benefits letter / statement

- Council Tax bill

Preferred method of communication:

Indicate how you wish to be contacted about the progress and outcome of your application. Unless you specify otherwise we will write to your current address.

Number of convictions:

Enter the total number of convictions that you are applying to have disregarded. You must complete a separate section B for each conviction. The word "conviction" includes a conviction, caution, warning or reprimand unless otherwise specified.

Signed .....

Date .....

Section B: Conviction details

Your stated personal details at the time of conviction (if different):

Forename(s) .....

Surname: .....

Date of Birth: .....

Armed Forces service number (if applicable):

Service No .....

Your stated address at the time of conviction (if different):

Property No. / name: .....

Street / Road: .....

Town / City: .....

County: .....

Postcode: .....

Details of the conviction you are applying to have disregarded:

Date of arrest: .....

Date of charge (if different): .....

Offence for which convicted: .....

Relevant police force / station: .....

Type of disposal: conviction*/ caution* / warning* / reprimand* (*delete)

If cautioned, which police station / date: .....

If convicted, which court / date: .....

Court Criminal Record Case No .....

Additional Information:

I am* / am not* (*delete) attaching copies of further materials / documentation in support of my application.

If you are submitting copies of further materials / documentation, please list them below:

.....

.....

.....

Former personal details:

If different from those recorded in section A, enter details of any other forename(s), surname(s) or date of birth that you may have used at the time the offence was committed.

Armed Forces service number:

If the conviction you are applying to have disregarded relates to a service offence and / or occurred whilst you were in the Armed Forces, enter your Armed Forces service number. This will assist the Ministry of Defence in locating relevant records.

Former address details:

If different from the details recorded in section A, enter details of your address, including postcode, at the time the offence was committed.

Details of your conviction:

Enter as much detail as you are able to remember about the circumstances of your arrest and conviction. The more detail you are able to provide, the more quickly we are likely to be able to identify and consider all relevant records.

The word "conviction" includes a conviction, caution, warning or reprimand unless otherwise specified.

Additional Information:

You may submit copies of additional materials and documentation in support of your application. Please note that you should not send originals as we are unable to return additional materials and documents to you. If you are submitting additional papers, please list them here.

Circumstances of the offence:

In order for the Home Secretary to assess whether your application meets the criteria set out in the Protection of Freedoms Act 2012, please provide concise details of the circumstances of the original offence that you were convicted of. Please indicate if you were made subject to any police notification arrangements.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

I confirm that, to the best of my knowledge, the conviction that I am here applying to have disregarded under the provision of Chapter 4 of Part 5 of the Protection of Freedoms Act 2012 related to an offence committed by two or more consenting parties who were, at the time of the offence, aged 16 or over. I also confirm, to the best of my knowledge, that the conviction that I am here applying to have disregarded does not relate to an offence committed in a public lavatory (which continues to be an offence under section 71 of the Sexual Offences Act 2003). I understand that information I provide in support of my application will be checked against police and other official records.

Signed: .....

Date: .....

Thank you for completing this form. Please now return it, along with copies of your identity credential and address verification, and any other supporting materials or documentation, to:

Chapter 4 Applications, SPPU, 4th Floor Fry Building, 2 Marsham Street, London, SW1P 4DF

Or by e-mail to chapter4applications@homeoffice.gsi.gov.uk

Appendix 3: A list of key organisations involved in the police records system

A range of organisations have a role in setting policy in relation to the management of police information. Below is a quick guide to each organisation, their role and the key documents published by them, and referred to throughout this guide.

Organisation	Form of Organisation	Role	Key Publications
Home Office (HO)	Government Department	The Home Office exercises its statutory power to issue guidance on the management of police records. The Home Office produces a new set of Counting Rules[250] on an annual basis. They are the only body to issue statutory guidance to police on disclosure.	1. Statutory Disclosure Guidance to chief police officers; 2. Home Office Counting Rules (HOCR); 3. Home Office Filtering Rules; 4. National Crime Recording Standard; 5. National Standard on Incident Recording; 6. Code of Practice on the Management of Police Information (MOPI)[251] 7. Guidance on the Rehabilitation of Offenders Act 1974. 8. Code of Practice on Management of Police Information
Standards and Compliance Unit (SCU)	Voluntary arrangement between disclosure bodies including local police forces and DBS[252].	The SCU draft and publish the Quality Assurance Framework (QAF). The SCU advise disclosure units on best practice but do not intervene in individual cases or direct disclosure units.	1. An applicant's introduction to the decision-making process for Enhanced Disclosure and Barring Service checks 2. QAF Method Products (MPs); 3. QAF Audit Trails (ATs); 4. QAF Sexting Guidance. Note: latest version of all QAF publications is version 9

[250] See the Home Office Counting Rules in detail at section 3.1

[251] This guidance was drafted by the National Centre for Policing Excellence.

[252] Overview Document1: overview of the Quality Assurance Framework. September 2014 (version 9)

Organisation	Form of Organisation	Role	Key Publications
		The SCU have produced a guidance document for individuals on what to expect from an application for a criminal records check. According to the SCU, this guidance is up to date and reflects changes to statute, government guidance and case law[253].	
Disclosure and Barring Service (DBS)	Government Agency	The DBS are responsible for receiving and processing applications to check against an individual's criminal records. They produce the Code of Practice for Disclosure and Barring Service Registered Persons which sets out the practices that an organisation making applications for criminal records checks must follow.	1. DBS Checks: guidance for employers 2. Code of Practice for Disclosure and Barring Service Registered Persons
National Police Chief's Council (NPCC).	Collaborative organisation between Police forces. Legally it is a "national unit hosted by the Metropolitan	The NPCC is responsible for skills sharing and objective setting between police forces.	1. 'The Guide to the Deletion of Information from National Police Systems'

[253] SCU: An applicant's introduction to the decision-making process for Enhanced Disclosure and Barring Service checks page 3

Organisation	Form of Organisation	Role	Key Publications
	Police Service[254]".		
College of Policing	Professional body for members of policing services. The body was created as a limited corporation but now exists as a statutory body.	The College of Policing is intended to work with those in the police force as an educator to improve knowledge, skills and performance independently of government.	1. Briefing note 'Police action in response to youth produced sexual imagery('Sexting')' 2. 'Authorised Professional Practice: Information management Retention, review and disposal'

[254] NPCC Frequently Asked Questions web page: http://www.npcc.police.uk/About/QuestionsandAnswers.aspx

Alex Temple is a Trainee Solicitor at Just for Kids Law. He has worked extensively on challenges to the keeping and sharing of police records. These include strategic cases challenging government policy in the appeal courts. He has worked with schools and police organisations to improve their practices and has undertaken research into the national state of police records management in relation to young people. His traineeship is funded by the Legal Education Foundation.

Just for Kids Law is a UK charity that works with and for children and young people to hold those with power to account and fight for wider reform by providing legal representation and advice, direct advocacy and support, and campaigning to ensure children and young people in the UK have their legal rights and entitlements respected and promoted. We help young people navigate their way through challenging times through our unique model of working with individual children and young people which combines direct advocacy and development opportunities with legal advice and representation. Just for Kids Law has gained a reputation for taking the evidence from our direct work with individual children and young people to fight for wider reform through strategic litigation and empowering children and young people to campaign. We also draw on our evidence to equip practitioners to work for children's rights and provide them with advice and expertise. Our Youth Justice Legal Centre has been at the forefront of training lawyers in representing children in court. Furthermore, we lead on monitoring compliance with human rights across the voluntary sector by hosting the Children's Rights Alliance for England.

Standing up for kids
JUST FOR KIDS LAW

Just for Kids Law
T: 020 3174 2279 | F: 020 7681 1393
Unit 4D, Leroy House, 436 Essex Rd, London N1 3QP
www.justforkidslaw.org | info@justforkidslaw.org