Building the picture

An inspection of police information management

July 2015

ISBN: 978-1-78246-817-2

www.justiceinspectorates.gov.uk/hmic

Contents

Glossary

ACPO	Association of Chief Police Officers
Association of Chief Police Officers	professional association of police officers of assistant chief constable rank and above, and their police staff equivalents, in England, Wales and Northern Ireland; led and co-ordinated operational policing nationally; a company limited by guarantee and a statutory consultee; its president was a full-time post under the Police Reform Act 2002; replaced by the National Police Chiefs' Council on 1 April 2015
APP	Authorised Professional Practice
Authorised Professional Practice on information management	official source of professional practice on police information management, approved by the College of Policing, to which police officers and staff are expected to have regard in the discharge of their duties
chief officer	in police forces outside London: assistant chief constable, deputy chief constable and chief constable; in the Metropolitan Police Service: commander, deputy assistant commissioner, assistant commissioner, deputy commissioner and commissioner; in the City of London Police: commander, assistant commissioner and commissioner; includes a member of police staff who holds equivalent status to a police officer of these ranks

Code of Practice	code relating to the discharge of their functions by chief officers; issued by the College of Policing, with the approval of the Home Secretary, under section 39A, Police Act 1996; the College may do this if it considers that it is in the national interest to do so, or if it considers it is necessary in the interests of the promotion of efficiency and effectiveness of police forces generally or to facilitate joint or co-ordinated operations by any two or more police forces; chief officers are required to have regard to any such code of practice in discharging functions to which the code relates; see further information on evolution of national guidance in Annex B
Code of Practice on the Management of Police Information 2005	code issued in 2005 by the National Centre for Policing Excellence (since replaced by the College of Policing) under sections 39 and 39A, Police Act 1996 and sections 28, 28A, 73 and 73A, Police Act 1997
College of Policing	professional body for policing in England and Wales, established to set standards of professional practice, accredit training providers, promote good practice based on evidence, provide support to police forces and others in connection with the protection of the public and the prevention of crime, and promote ethics, values and standards of integrity in policing; its powers to set standards have been conferred by the Police Act 1996 as amended by the Anti-social Behaviour, Crime and Policing Act 2014; under section 40C, Police Act 1996, the Home Secretary has power to direct the College, requiring it to exercise any statutory function vested in the College, and to carry out such other duties for the purpose of furthering the efficiency, effectiveness or integrity of the police as the Home Secretary specifies
data quality principles	principles with which all police information must conform; includes the principles that data must be accurate, adequate, relevant and timely

HOLMES	Home Office Large Major Enquiry System
Home Office Large Major Enquiry System	information management system used to host information about major crime investigations; used by every UK police force to support the investigation of murders and a variety of other major crime investigations and major incidents
intelligence	defined in Authorised Professional Practice as “collected information that has been developed for action”; all intelligence is therefore information, but not all information is categorised as intelligence; information may be categorised as intelligence and vice-versa; individual pieces of information and intelligence therefore need to be reviewed on a regular basis to ensure that their categorisation remains appropriate to the circumstances
national guidance on the management of police information	detailed guidance defining the information management standards required within forces; supports the Code of Practice on the Management of Police Information 2005; current (2015) version is the third edition of this guidance; part of the Authorised Professional Practice on information management approved by the College of Policing
National Intelligence Model	method of working based on the principles of problem-solving policing and the use of community and criminal intelligence; the ACPO (2005) Code of Practice on the National Intelligence Model, issued in January 2005 by the Home Secretary under the Police Reform Act 2002, provides the statutory basis for its introduction

National Police Chiefs' Council	organisation which brings together 43 operationally independent and locally accountable chief constables and their chief officer teams to co-ordinate national operational policing; works closely with the College of Policing, which is responsible for developing professional standards, to develop national approaches on issues such as finance, technology and human resources; replaced the Association of Chief Police Officers on 1 April 2015
national policing lead	senior police officer with responsibility in England and Wales for leading the development of a particular area of policing
National Retention Assessment Criteria	framework used for making decisions about whether or not information needs to be retained for a policing purpose; criteria for this include known risk factors, necessity and proportionality; part of the Authorised Professional Practice on information management approved by the College of Policing
National Special Branch Intelligence System	information management system used to host information and intelligence gathered in the course of counter-terrorism investigations
NPCC	National Police Chiefs' Council
NRAC	National Retention Assessment Criteria
PND	Police National Database
Police National Database	national IT system that allows the police service to share access to and search local force information on a national basis; designed to provide forces with immediate access to up-to-date information drawn from local crime, custody, intelligence, child abuse and domestic abuse systems

Executive summary

Her Majesty's Inspectorate of Constabulary (HMIC) is an independent inspectorate with a statutory responsibility to "inspect, and report on the efficiency and effectiveness of every police force maintained for a police area" in England and Wales.[1]

This report sets out findings from our review of the business processes police forces in England and Wales use to collect, record, process, evaluate and share information.

Why information management is important

Information[2] is the lifeblood of the police service. It leads to effective investigations, timely arrests and appropriate criminal justice outcomes. It also helps to prevent further crimes being committed. Information is vital in the fight against crime.

Seemingly one-off instances of suspicious or criminal behaviour assume a greater importance if it can be shown, by linking information, that they are not isolated, but form a pattern of behaviour that gives rise to concern. The whole picture may well be greater than the sum of its parts. This is why linking information and building the picture of the crime are so important – and why the consequences of failing to make the right links can have a significant adverse impact on the public; for example, the mistakes that were made during the police handling of allegations against Jimmy Savile. This is discussed in more detail below.

The recent decision of the Supreme Court in *R (Catt) v Association of Chief Police Officers* [2015][3] emphasises the pivotal importance of complying with the Code of Practice on the Management of Police Information 2005, the associated Authorised Professional Practice (APP) on information management[4] and the former editions of

[1] Section 54(2) of the Police Act 1996.

[2] In this report, 'information' is used to refer to both information and intelligence. See page 19.

[3] *R (Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland and another (Equality and Human Rights Commission and others intervening)* [2015] UKSC 9.

[4] *Authorised Professional Practice on information management*, College of Policing, 2013. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/ This is the body of guidance published by the College of Policing to provide the police service in England and Wales with policy and procedures to follow.

the national guidance.[5] In her judgment, Baroness Hale echoes one of the main themes of this report in stating: “We do not need any reminding, since the murder of two little girls by a school caretaker in Soham and the recommendations of the report of the Bichard Inquiry which followed (2004) (HC 653), of the crucial role which piecing together different items of police intelligence can play in preventing as well as detecting crime.”[6]

In the *State of Policing* report published by HMIC on 27 November 2014[7], we stated:

> "The oxygen of effective policing is information, but it is useless if it cannot be found and used at the time and in the circumstances in which it is needed. And in policing, if it is inaccessible to those who need it, great harm may occur which could and should have been prevented. Police forces do not compete with one another. Information about a person, vehicle, weapon or address does not belong to any one force. It is essential that the systems which police forces use for the recording and dissemination of information are as efficient and effective as possible. And that means that the information needs to be where it is needed, when it is needed.”
>
> "It remains a matter of very serious concern that progress in ensuring the interoperability of police systems of information and communications technology has been as slow, insular and isolationist as it has. Until the police have a fully-functional interoperable system of networks, public safety is imperilled and lives are at risk."

In the *State of Policing* report published on 31 March 2014[8], we said:

> "It is … important that, with the needs to make savings through more efficient working, the police service accelerates its acquisition and use of common digital devices and systems which enable it to acquire, analyse and disseminate information which is necessary for the protection of the public and the apprehension and prosecution of offenders, and provide the public with better access to policing services. The state of information and communications technology in too many police forces remains quite

[5] Code of Practice on the Management of Police Information issued under sections 39 and 39A, Police Act 1996 and sections 28, 28A, 73 and 73A of the Police Act 1997. Available from http://library.college.police.uk/docs/homeoffice/codeofpracticefinal12073.pdf

[6] *Ibid*, para 48.

[7] *State of Policing: The Annual Assessment of Policing in England and Wales 2013/14,* HMIC, London, November 2014. Available from www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/state-of-policing-13-14.pdf

[8] *State of Policing: The Annual Assessment of Policing in England and Wales 2012/13,* HMIC, London, March 2014. Available from www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/2014/03/state-of-policing-12-13.pdf

inadequate and, in some cases, primitive. It is essential that the advances of the forces with the best technology – such as Cambridgeshire, Nottinghamshire, Hampshire and South Wales – are adopted and then improved upon by all, working more than ever as one police service rather than 43."

"In this respect, for too long the police service has lagged far behind the private sector, to the advantage of offenders and the hazard of the public. This must change, and the needs of the public to be protected against long-established crimes as well as those made possible or easier by the internet and its associated capabilities, make it urgent. This is equally true in relation to the needs of the police service to continue to make significant improvements in the efficiency and effectiveness of what it does. If the utilities, financial services providers, retailers and other commercial organisations can gather, analyse, understand and ensure the efficient, secure communication of information in pursuit of profit, the police – even though they are not nearly to the same extent in control of their environment and are dealing with incomplete and sometimes unreliable information – must be able to do so in pursuit of something far more important."

Background: "*Mistakes Were Made"*

On 12 March 2013, HMIC published the findings of a review into how the Metropolitan Police Service, Surrey Police and Sussex Police dealt with the information and allegations which they received between 1964 and 2008 regarding the criminal sexual conduct of the late Jimmy Savile.[9]

This review considered the way in which these forces applied the Code of Practice on the Management of Police Information 2005, the APP on information management[10] and the former editions of the national guidance[11] in dealing with the information and allegations. It also examined the extent to which those forces made

[9] *"Mistakes Were Made" - HMIC's review into allegations and intelligence material concerning Jimmy Savile between 1964 and 2012,* HMIC, March 2013. Available from www.justiceinspectorates.gov.uk/hmic/media/review-into-allegations-and-intelligence-material-concerning-jimmy-savile.pdf

[10] *Authorised Professional Practice on information management*, College of Policing, 2013. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/ This is the body of guidance published by the College of Policing to provide the police service in England and Wales with policy and procedures to follow.

[11] *Guidance on the Management of Police Information*, 1st edition, Central Police Training and Development Authority, 2006, produced by the National Centre for Policing Excellence, and the second edition of the same, produced by the National Policing Improvement Agency in 2010. It is referred to in this report as 'national guidance'.

effective use of the Police National Database[12] to aggregate discrete pieces of information (from within and across forces) and so build a picture of the extent and nature of the alleged offending.

HMIC concluded that mistakes had been made in the handling of information and allegations and stated that we were “sufficiently concerned about information management" to conduct a further review in this area. This inspection fulfils this commitment and answers the question: could the same mistakes be made again?

Methodology

Our principal inspection objectives were to establish:

- if force strategies, policies and procedures for information management adhere to the principles of the APP on information management and former editions of the national guidance, are proportionate to risk and fit for purpose;
- if information and intelligence are captured, recorded, evaluated, acted upon, audited and retained by the police (including safeguarding interventions) in an effective way; and
- if the use of the Police National Database is effective and efficient.
- To answer these questions, HMIC analysed the results of a self-assessment survey[13] of information management practices which was completed by all 43 forces in England and Wales in 2013 (to give an indication of the national picture), and conducted three days of fieldwork in each of 13 forces.
- A full methodology (including the criteria used in deciding the forces visited for the fieldwork stage of the inspection) is given on page 17.

Findings

Given that chief constables are obliged to have regard to the Code of Practice on the Management of Police Information 2005, we expected that either:

[12] The Police National Database is a national information management system that improves the ability of the police service to manage and share information, to prevent and detect crime and make communities safer. It offers a capability for the police service to share, access and search local information electronically, overcoming artificial geographical and jurisdictional boundaries.

[13] This survey was commissioned by the ACPO Information Management Business Area Lead, and conducted on his behalf by the College of Policing. We are grateful for permission to use the results.

- they would ensure that their forces complied with the Code, and with the relevant section of the APP on information management or former editions of the national guidance;[14] or

- if, because of their local context and operating environment, they decided not to comply with elements of the APP on information management or former editions of the national guidance, that proper records would be maintained about the extent of and rationale for any move away from the Code.

We were therefore disappointed to find that the reasons for decisions to depart from the APP on information management or former editions of the national guidance were only recorded in three of the 13 forces we inspected.

We also expected each force to have in place a current information management strategy – a requirement stipulated in the Code of Practice on the Management of Police Information 2005. Again, we were disappointed to find that this was not always the case.

In the light of case law and high-profile cases such as Jimmy Savile's long period of sex offending, we are materially concerned about the extent to which the police service is responding fully to the responsibilities inherent in a changing environment, where speedy access to up-to-date and relevant information is essential. For example, we found cases where forces had not revisited their position since the whole of the police service completed local information management implementation plans in 2010. In this regard, the absence of appropriate audit and assurance regimes (to check that information is being appropriately assessed, retained or disposed of) is especially worrying, and needs to be addressed swiftly.

HMIC found that forces which maintained a central information management team were better able to adopt the principles of the APP on information management and former editions of the national guidance. This was especially so when those teams had access to an integrated computer system that was able to reference and facilitate the assessment of all the information held on a named individual without the need to search separate computer systems.

It is a matter of serious concern that there is insufficient review taking place of the information that forces hold. Without these reviews – and the means to demonstrate that they have taken place properly or at all – the police service leaves itself vulnerable to challenge. The absence of sound and consistent reviews means that information might be destroyed when it should be kept, thus increasing the risk to public safety.

[14] *Authorised Professional Practice on information management*, College of Policing, 2013. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/ This is the body of guidance published by the College of Policing to provide the police service in England and Wales with policy and procedures to follow.

The volume of information acquired by the police means that not every piece of information can be evaluated and processed at the same time. The question then arises of how to identify those pieces of information which demand more immediate consideration than others. Clearly, the information which informs the police of a greater or more immediate risk to the public should be considered as soon as possible. We found that the extent to which information was reviewed, prioritised and indexed – and the capacity to undertake this exercise – varied between and within forces.

A significant strand of our inspection examined how sensitive information[15] is handled, particularly when it is acquired and held as a result of specialist policing activities such as major crime investigations, counter-terrorism investigations and internal investigations of police officers and staff for misconduct, or corruption or other criminal offences. We found that there is scope for better integration between the IT systems which house sensitive information and the mainstream databases available to the police (such as the Home Office Large Major Enquiry System[16]). There is also scope for more effective processes to transfer information between systems; while our inspection found some awareness of the problems caused by the lack of such processes (for instance, some forces are developing the means to identify, isolate and transfer appropriate records on a case-by-case basis), there is more to be done.

Where information is marked as sensitive, the police must undertake reviews from time to time to determine whether such a classification remains appropriate. The importance of information fluctuates with the passing of time, and the police service should do more to act on those fluctuations. We found evidence that different practices are being followed in the 43 police forces in England and Wales with regard to the handling of sensitive information.

We were also concerned to note that only four of the forces we visited had a force-wide policy setting out how sensitive information should be treated; and even in those four forces, we did not find any evidence to show that compliance with the policy was being monitored to ensure that it was being followed. The absence of consistent practice together with differences of approach in implementation results compromises the ability to manage information effectively.

[15] 'Sensitive information' is that which is contained in specialist business areas, and generally hosted and used outside mainstream policing intelligence systems and processes. It is therefore only available to specialist officers. Examples include information on current operations; major crime investigations or counter-terrorism information; and information held by professional standards directorates.

[16] An ICT system used for major crime investigations.

As a result of these findings, we have made ten recommendations (for the Home Office; the national lead for information management business area; chief constables and the College of Policing). These are set out on page 63.

Conclusions

Given the way in which the police service has responded to the need to manage information more effectively, could the tragedy of errors made in sharing information that occurred in Savile be repeated today?

We have found that the police service as a whole is mindful of the need to improve how it deals with the mass of information which it acquires every day.

The task, however, is a substantial one.

It would be unrealistic for the police service to make categorical assurances that the risk posed by predatory offenders could be eradicated on the sole basis of improvements in the management of police information. Nevertheless, there is a real and pressing need for greater attention to be paid to the management of police information, so that greater consistency is achieved across all forces. It is not enough that some forces manage information better than others. The purpose of a national system is to ensure that, as far as possible, relevant information is available to the right person at the right time, no matter in what part of the country that piece of information was generated.

It may have been necessary initially to allow the exercise of local discretion to adjust management information practices to get the system up and running, particularly in the absence of a comprehensive IT solution. But in today's environment, local variations in practice carry real risks that the mistakes we identified in our report about police contact with Jimmy Savile could be repeated.

Greater rigour in the implementation of management information policies is required so that all forces are brought up to the standards of the best.

Introduction

This report details findings from our review of the processes that police forces in England and Wales use to collect, record, process, evaluate and share information.

Background: "*Mistakes Were Made*"

In 2013, HMIC published its findings of a review into how the Metropolitan Police Service, Surrey Police and Sussex Police dealt with the information and allegations about the criminal sexual conduct of the late Jimmy Savile which they received between 1964 and 2008.[17]

This review looked at the way in which these forces applied the statutory Code of Practice on the Management of Police Information (and the associated national guidance which was issued as a result of that code) in dealing with the information and allegations. It built a picture of the extent and nature of the alleged offending and also examined the extent to which those forces made effective use of the Police National Database[18] to aggregate discrete pieces of information (both within and across forces).

The report concluded that mistakes had been made in handling information. This failure to connect the various allegations was critical to the eventual outcome of investigations. Information had been available, but not linked together, in four separate investigations. This failure to 'join the dots' inhibited a full understanding of Savile's criminality. As a result, the potential for further investigation and prosecution of Savile was missed.[19]

The errors that took place in the case of Savile straddled the introduction of systems and procedures which were put in place following the report of the Bichard Inquiry.[20] This suggests that lessons were not adequately learned from the latter in time to investigate and deal appropriately with the former.

---

[17] Available from www.justiceinspectorates.gov.uk/hmic/media/review-into-allegations-and-intelligence-material-concerning-jimmy-savile.pdf This review also examined whether West Yorkshire Police, as the force area in which Savile lived for most of his life, received details of this information and these allegations.

[18] *Code of Practice on the Operation and Use of the Police National Database,* made by the Home Secretary, March 2010, under section 39A, Police Act 1996.

[19] *"Mistakes Were Made" - HMIC's review into allegations and intelligence material concerning Jimmy Savile between 1964 and 2012,* HMIC, March 2013, chapter 9. Available from www.justiceinspectorates.gov.uk/hmic/media/review-into-allegations-and-intelligence-material-concerning-jimmy-savile.pdf

[20] The report resulting from Lord Bichard's enquiry into the vetting procedures which allowed child murderer Ian Huntley to be employed as a school caretaker. *The Bichard Inquiry report*, House of Commons, HC653, June 2004.

In our report about Savile we stated that because we were "sufficiently concerned about information management and its wider effect on records contained on [the Police National Database]",[21] we would conduct a further review in this area. This inspection fulfils that commitment.

This report also fulfils HMIC's obligation to monitor compliance with the Code of Practice on the Management of Police Information, associated guidance and standards.[22]

About this inspection

Objectives

Our terms of reference reflected the concerns that we identified in our report about Savile[23] and are set out in full at Annex A.

In summary, our objectives were to establish:

- if force strategies, policies and procedures for information management adhere to the principles of the APP on information management and former editions of the national guidance, are proportionate to risk and fit for purpose;
- if information and intelligence are captured, recorded, evaluated, acted upon, audited and retained by the police (including safeguarding interventions) in an effective way; and
- if the use of the Police National Database is effective and efficient.

Scope

The volume of information which the police service collects and retains is vast. No single inspection can ever properly consider the performance of forces with regard to every piece of information that they amass, and so we have borne in mind what

[21] *"Mistakes Were Made" - HMIC's review into allegations and intelligence material concerning Jimmy Savile between 1964 and 2012,* HMIC, March 2013, para 8.21. Available from www.justiceinspectorates.gov.uk/hmic/media/review-into-allegations-and-intelligence-material-concerning-jimmy-savile.pdf

[22] *Code of Practice on the Management of Police Information*, prepared by the National Centre for Policing Excellence, 2005, para 1.3.1 states that: "HM Inspectors of Constabulary will monitor police forces' compliance with this Code, associated guidance, and standards".

[23] *"Mistakes Were Made" - HMIC's review into allegations and intelligence material concerning Jimmy Savile between 1964 and 2012,* HMIC, March 2013. Available from www.justiceinspectorates.gov.uk/hmic/media/review-into-allegations-and-intelligence-material-concerning-jimmy-savile.pdf

prompted HMIC to undertake this inspection: the information that should have been collected, retained, considered and disseminated about Savile.[24]

Therefore, we have limited our examination to the management of police information in this context. We have considered the extent to which police forces have adopted the framework of national guidance and implemented it within local policies.

We have not examined how the police service treats photographs or biometric records, as these are outside the scope of our inspection.

However, we have examined the process by which the police deal with information from specialist policing activities – primarily major crime investigations, counter-terrorism and those relating to the internal investigation of police staff for misconduct, corruption or criminal offences – within the context of our findings on Savile.[25]

Methodology

HMIC analysed the results of a self-assessment survey on the management of information which all forces completed in September 2013[26] and conducted fieldwork in 13 police forces.

The selection of forces for fieldwork was based on three criteria:

- involvement in cases reported by victims of Savile (Surrey Police, Sussex Police, the Metropolitan Police Service and West Yorkshire Police);
- involvement in the Bichard Inquiry[27] (Cambridgeshire Constabulary and Humberside Police); or
- because there was a high, low or average (compared to other forces in England and Wales) level of risk regarding information management identified in the national self-assessment survey (Dyfed Powys Police, Hampshire Constabulary, Lancashire Constabulary, Lincolnshire Police, Merseyside Police, North Yorkshire Police and Nottinghamshire Police).

---

[24] *"Mistakes Were Made" - HMIC's review into allegations and intelligence material concerning Jimmy Savile between 1964 and 2012,* HMIC, March 2013, chapter 8. Available from www.justiceinspectorates.gov.uk/hmic/media/review-into-allegations-and-intelligence-material-concerning-jimmy-savile.pdf

[25] *Ibid,* chapter 8.

[26] This survey was commissioned by the ACPO national policing Information Management Business Area lead because of the failures in this area identified in HMIC's report "*Mistakes Were Made".* It was conducted by the College of Policing.

[27] The report resulting from Lord Bichard's enquiry into the vetting procedures which allowed child murderer Ian Huntley to be employed as a school caretaker. *The Bichard Inquiry report*, House of Commons, HC653, June 2004.

The fieldwork examined:

- how information is recorded, reviewed, retained and deleted in each force;
- the quality of data supplied to the Police National Database, and whether that data was supplied and refreshed in a timely fashion;
- the process for inclusion and handling of sensitive information;[28] and
- the ability of the force to automate the process of linking police information and intelligence data, in line with the APP on information management and former editions of the national guidance.

Our findings are based on:

1. interviews with over 180 relevant police officers and staff throughout the forces we visited; and
2. the information provided by the national self-assessment survey. We were able to test what we were told by sitting alongside those who assess and link pieces of information to determine the intelligence value. We spoke to a number of trained operators on the Police National Database.

Our fieldwork was undertaken between May and August 2014 in 13 police forces within England and Wales, following a pilot inspection in one force area.

The police forces which we inspected comprise 45.2 percent of the total police workforce across England and Wales (as at 31 March 2014)[29] and deal with 44.8 percent of the crime reported in the year to 31 March 2014 (excluding fraud).[30]

Structure of this report

We start the chapters relating to our findings with an overview of the national guidance, followed by an assessment of how, based on the national survey completed by forces themselves, the 43 police forces use databases (local and

[28] 'Sensitive information' is that which is contained in specialist business areas, and generally hosted and used outside mainstream policing intelligence systems and processes. It is therefore only available to specialist officers. Examples include information on current operations; major crime investigations or counter-terrorism information; and information held by professional standards directorates.

[29] *Police workforce, England and Wales, 31 March 2014*, Home Office, 17 July 2014. Available from www.gov.uk/government/publications/police-workforce-england-and-wales-31-march-2014/police-workforce-england-and-wales-31-march-2014

[30] *Crime in England and Wales, Year Ending March 2014*, Office for National Statistics, 17 July 2014. Available from: www.ons.gov.uk/ons/dcp171778_371127.pdf

national) to manage information, and how they have addressed the requirements of the APP on information management[31] in terms of people and structures.

Then, we have set out the findings from our inspection under the headings used in the APP on information management:

- collection and recording;
- evaluation;
- managing police information (common process);
- sharing police information; and
- retention, review and disposal.

Because the management of sensitive information was a particular issue identified in *"Mistakes Were Made"*, this is considered separately in the last chapter.

A note on terminology: information or intelligence?

The APP on information management defines intelligence as "collected information that has been developed for action". It may also be classified as "confidential" or "sensitive".[32] Thus in policing terms, not all information is classified as intelligence, but all intelligence is a form of information. Although the words "information" and "intelligence" are commonly used interchangeably within the police service, there is a distinction which determines how they are treated.

In order to categorise the information which is received, the police service has devised procedures to distinguish "information" from "intelligence". For example, the police officer who is simply informed that a person lives at a certain address without any suggestion that that person is a victim or perpetrator of a crime may treat that knowledge as information. However, that information might need to be reclassified as intelligence if it becomes known that the premises where that person lives have been raided several times on suspicion of being a place where illegal drugs or stolen goods are stored.

There can be movement between the two categories of information and intelligence. Similarly, the importance or sensitivity of some intelligence may ebb and flow depending on its nature. For example, intelligence that is pertinent to an ongoing

31 *Authorised Professional Practice on information management*, College of Policing, 2013. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/ This is the body of guidance published by the College of Policing to provide the police service in England and Wales with policy and procedures to follow.

32 *Intelligence management*, Authorised Professional Practice, College of Policing, October 2013. Available from www.app.college.police.uk/app-content/intelligence-management/?s

police operation may be classified as sensitive during the course of that operation. However, its sensitivity diminishes once the police operation concludes. Similarly, intelligence which suggests that a crime is to be committed on a certain day may lose its value if that day passes and nothing untoward takes place.

This suggests strongly that the categorisation of information and intelligence is a fluid process and that individual pieces of information and intelligence need to be reviewed on a regular basis to ensure that their categorisation remains appropriate to the then current circumstances.

For the purpose of this report, unless otherwise indicated both information and intelligence are referred to as information.

Recent developments in information management: Operation Hydrant

We conclude our introductory remarks by acknowledging the efforts which the police service is making on one of HMIC's clear conclusions in its report into Savile.[33] There, we stated the following:

> "[i]t is absolutely clear to us as a result of [the Savile] review that one of the reasons why allegations were not made at the time or investigations were not conducted as they might have been centres on Savile's status. He was a well-known national celebrity, praised for his substantial fund-raising efforts, and a household name to many…
>
> We wonder, as a result, whether those responsible for investigating potential criminal offences have a different approach to dealing with investigations about those in the public eye."[34]

Since HMIC's report was published, the police service has set up an initiative, known under its operational name, Hydrant. The aim of this initiative is to co-ordinate nationally investigations into historic allegations of child abuse within institutions or where the offender is believed to be a person of public prominence, such as an elected official, a celebrity, a person of significant national prominence, or a person otherwise in the public eye. Although this initiative is relatively new, this coordinated approach should help the police service to reduce the risk of failures in making the right links across pieces of information about high-profile individuals which need to be acted upon in the future.

---

[33] *"Mistakes Were Made" - HMIC's review into allegations and intelligence material concerning Jimmy Savile between 1964 and 2012,* HMIC, March 2013. Available from www.justiceinspectorates.gov.uk/hmic/media/review-into-allegations-and-intelligence-material-concerning-jimmy-savile.pdf

[34] *Ibid,* paras 12.38-39.

Why information management matters

Every day of the year, the 43 police forces in England and Wales receive millions of separate pieces of information. They may concern victims of crime, those suspected of committing crime or the crime itself. They may relate to crimes already committed, those which are actually in the process of being committed or those which are to take place in the future. They may come from members of the public performing a civic duty in helping the police, from associates of those who commit crime, from a worried relative whose purpose is to prevent his loved one from breaking the law, from enquiries which police officers have instigated or even from anonymous sources.

Collectively, the police service has to decide how to treat these separate pieces of information, so that the most important, serious or urgent are assessed, retained and, where appropriate, acted upon, either alone or in conjunction with other information that may relate to the same individual or crime. All this has to be done in a timely fashion.

This task is not a simple one. It is easy with hindsight to identify the one clue about a person's guilt that is hidden among long and sometimes rambling lists of accusations.

Rightly, the public expects that the police service will work together to use modern technology to ensure that such information is properly considered, appropriately retained and readily accessible. Today, it is not unreasonable to expect that relevant information received by an officer in one police station or on the beat in one part of a police force will be made available to other officers, as necessary, in England and Wales within an acceptable period of time.

If someone carries out crimes and is able to cross police force borders and move from one end of England and Wales to the other within a day, and carry out further crimes, it is not unreasonable to expect that information about the crimes is shared between forces. Then there is a realistic prospect that further crimes might be thwarted and a criminal apprehended. It can no longer be acceptable that an individual is able to carry out a series of offences simply because information that may have led to his or her arrest is left in the records retained by one force which has not told others about the information that it has received.

The move more generally towards intelligence-led policing reinforces the importance of effective management of information regarding potential criminals and criminal activity. If that information is not handled correctly, crimes which may have been prevented are committed; and criminals who may have been apprehended before causing any harm are allowed to carry on their unlawful enterprise, creating victims and anguish for those who suffer at their hands.

This emphasises the need for the 43 police forces of England and Wales to ensure that they gather, collate, assess, retain and share information and intelligence in a timely, consistent and comprehensive way.

National guidance on information management

In 2005, the Home Secretary issued a Code of Practice on the Management of Police Information.[35] In 2006, the Central Police Training and Development Authority produced, on behalf of the Association of Chief Police Officers, Guidance on the Management of Police Information, which was published by the National Centre for Policing Excellence. This was revised in 2010 by the National Policing Improvement Agency, resulting in the publication of a second edition.

That guidance has now been superseded by the APP on information management, which was published in October 2013.[36] A brief overview of the evolution of the national guidance on the Code of Practice on the Management of Police Information 2005 is set out in Annex B.

Following the guidance: the impact of variations in practice

The policy and procedures set out in APP on information management provide a blueprint which, if followed, ensures that the same approach to managing information is adopted throughout the 43 police forces of England and Wales.

However, we have concerns about the extent to which chief officers are obliged to follow precisely the guidance set out in that APP.

The Code of Practice on the Management of Police Information states that:

> "[c]hief officers of police must … ensure that their forces adopt practices for the management of information that ensure such information is used effectively for police purposes and in compliance with the law."

35 Code of Practice on the Management of Police Information issued under sections 39 and 39A, Police Act 1996 and sections 28, 28A, 73 and 73A of the Police Act 1997. Available from http://library.college.police.uk/docs/homeoffice/codeofpracticefinal12073.pdf

36 *Authorised Professional Practice on information management*, College of Policing, 2013. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/ This is the body of guidance published by the College of Policing to provide the police service in England and Wales with policy and procedures to follow.

It goes on to state that:

> "[t]he purpose of [the] Code is to ensure that there is broad consistency between forces in the way information is managed within the law, to ensure effective use of available information within and between individual forces and other agencies, and to provide fair treatment to members of the public."

The second edition of the Guidance on the Management of Police Information 2010 required each chief officer to "have regard to" the standards that were set out in the guidance.[37]

However, the guidance went on to recognise that: "chief officers are required to balance resources against local policing needs".[38] As a result, the guidance continued by stating:

> "[e]ach chief officer [was] afforded the flexibility to decide on the scale of implementation for each standard contained within the MOPI [Management of Police Information] Guidance, based on the individual structure, resources, priority, risk and the local needs of each force".[39]

As we have already detailed in this report, the only obligation set out in the APP on information management is for chief officers to have "overall responsibility" for their force's compliance with the Code of Practice on the Management of Police Information 2005.

The Code of Practice permits variations in practice at the risk of impairing effective and consistent information management regimes at local force level.

In "*Mistakes Were Made"* (which was written before the introduction of the APP on information management but is, in our judgment, still relevant), we considered this to be a major barrier to the successful implementation of the guidance.[40] This is because the margin of discretion appeared to revert to the position which Bichard identified, namely, that:

---

[37] *Guidance on the Management of Police Information*, 2nd edition, National Policing Improvement Agency, 2010, page 8.

[38] *Ibid*

[39] *Ibid*

[40] *"Mistakes Were Made" - HMIC's review into allegations and intelligence material concerning Jimmy Savile between 1964 and 2012,* HMIC, March 2013, para 8.4. Available from www.justiceinspectorates.gov.uk/hmic/media/review-into-allegations-and-intelligence-material-concerning-jimmy-savile.pdf

> "[e]ach of the 43 forces [is able to produce] its own set of local guidance and directions to give effect to ACPO's (and others') national guidance." [41]

We do not regard the position as satisfactory. All those involved in the management of police information should be clear about the extent of their duty "to give effect to ACPO's (and others') national guidance."

There must be greater consistency in the implementation of the APP on information management. Local variations in practice impede the ability of forces to "join the dots" effectively. The absence of modern technology in some forces represents a real impediment to designing efficient systems that improve compliance. However, more can and should be done to improve practice and we have made recommendations to address the inconsistencies we have found. We will return to this issue in later inspections to assess whether a requirement to comply with national guidance is necessary for the protection of the public.

We invite the Home Office to consider mandating the guidance, given the degree of variation we found.

Findings

We have adopted a robust approach to managing information in our inspection. As we have stated, the Code of Practice on the Management of Police Information 2005 specifically requires HMIC to "monitor police forces' compliance with [the] Code, associated guidance, and standards".[42] If forces diverge from the Code and the relevant section of the APP on information management, we expect chief constables to have compelling reasons why divergence is necessary. Decisions to do so may, in certain circumstances, compromise the ability of forces to track down the information officers need to fight crime effectively.

We were therefore disappointed to find that decisions to depart from the APP on information management or former editions of the national guidance were only recorded in three of the 13 forces we inspected.

Recommendation 1

> By 30 November 2015, chief constables should ensure that a review is undertaken of the way in which their forces' information management policies and practice comply with the APP on information management so that they give effect to the national approach and minimise any divergence from that APP.

[41] *The Bichard Inquiry Report*, House of Commons, HC653, June 2004, para 3.81.

[42] Code of Practice on the Management of Police Information 2005, para 1.3.1, states that: "HM Inspectors of Constabulary will monitor police forces' compliance with this Code, associated guidance, and standards".

Use of databases

Developments in information technology have made a substantial difference to the way in which separate pieces of information can be linked together. Advances in IT mean that databases containing millions of pieces of individual information can be searched easily, comprehensively and quickly. This is of enormous benefit to the police service. However, the usefulness of any database is limited by the accuracy and completeness of the information that is added to it.

This section provides an overview of some of the databases which the police service has created, and findings on the extent to which their use complies with the APP on information management.[43]

The APP on information management identifies the different ways in which the police may acquire information, and provides examples of the principal areas under which that information should be recorded, for example: domestic abuse, child abuse investigations and public protection. It clearly states: "Information from key business areas (for example, crime, intelligence, domestic abuse, child abuse and custody) should be uploaded onto the police national database (PND) on a regular basis."

All the information which a police force acquires should be handled in accordance with the guidance set out in the APP on information management, subject to any reasoned, local variation from it.

However, there remains the need to ensure that the most relevant information acquired locally is made available not only to the police force managing the information but also to colleagues in the remaining police forces in England and Wales. That information is divided into five subjects, which the police service refers to as business areas. These are: child abuse; domestic violence; records about an individual who is taken into police detention (these are referred to as 'custody records'); records of reported crime; and intelligence reports.

The 43 police forces in England and Wales may retain the information locally in either integrated or stand-alone information technology systems, or a combination of the two. Data from these systems about the five core subjects should be supplied to the Police National Database.[44] [45]

---

[43] *Authorised Professional Practice on information management*, *Collection and recording, recording,* College of Policing, 2013, para 2. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/collection-and-recording/#recording

[44] *Authorised Professional Practice on information management, Collection and recording, Recording,* College of Policing, 2013, para 2. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/collection-and-recording/#recording

The Police National Database

The Police National Database is a national IT system which improves the ability of the police service to manage and share information, to prevent and detect crime and make communities safer. It offers a capability for the police service to share, access and search local information electronically, overcoming artificial geographical and jurisdictional boundaries.[46]

It was launched in June 2011 and hosts copies of intelligence, information and local records which are created, managed and owned by police forces and law enforcement agencies. It is a powerful policing tool, containing in excess of 1.4 billion records and 15 million images.[47]

It is important to understand the relationship between the APP on information management and former editions of the national guidance, and the Police National Database:

- the guidance seeks to regulate the way in which the police service should handle the information which it acquires in terms of record creation; retention; access by others; and deletion; and
- the Police National Database does not create any records of its own: it serves to house those records created by police forces in accordance with the guidance. The quality of information supplied to the Police National Database from forces therefore has a direct result on the database's ability to match and identify critical information links. Where this is poor, incomplete or absent, the effectiveness of the Police National Database is compromised. The system can only be as effective as the records contained within it.

The Home Office Large Major Enquiry System (HOLMES)

In addition to the Police National Database, there is a separate information technology system which is used to host information about major crime investigations. This runs in parallel with the information about the five core subjects

---

[45] The Police National Database should not be confused with the Police National Computer, which holds details of convictions and wanted persons, among other things. Therefore, details of a person suspected of having committed or having been arrested for an offence but not convicted would be on the Police National Database, provided it is captured in a local record. If the person were convicted, details of the conviction would also feature on the Police National Computer.

[46] *Code of Practice on the Operation and Use of the Police National Database*, made by the Secretary of State for the Home Department, March 2010, para 1.1.

[47] The method used to calculate total records held within PND altered on 13 May 2014. These are the records contained within the system on that date.

that populate the Police National Database. This system is formally known as the Home Office Large Major Enquiry System, or HOLMES.

In June 2012, there were approximately 250,000 incidents recorded on the system, each with varying amounts of data. One incident alone accounted for 70,000 pieces of information.[48]

Guidance relating to major crime enquiries is contained in the Major Incident Room Standardised Administrative Procedures 2005, which state: "At all stages of the investigation, ensure timely dissemination of all intelligence gathered, making sure that it does not directly impact on the investigation (Recommendation 8, the Bichard Inquiry 2004)".[49] However, we found that the flow of information generated during a major crime enquiry could be significantly improved by ensuring the consistent and regular transfer of appropriate information to allow wider access to officers and staff.

Despite its status as a substantial database of information, HOLMES does not have any links to the Police National Database. As a result, unless a decision is taken to include appropriate information from HOLMES in the local force intelligence system, any information that is gathered as part of a major crime investigation will not be available via the Police National Database to other officers not directly associated to that major crime investigation.

We are concerned that, without such access, those who make enquires about individuals do not have all the information that is known collectively to the police service.

Recommendation 2

> By May 2016, the Home Office and National Police Chiefs' Council's Information Management Business Area lead, should agree and implement common standards to be used by forces to identify and transfer information, no longer sensitive to an enquiry contained within HOLMES, to systems which are accessible and searchable by the police service generally.

National Special Branch Intelligence System

In a similar way to HOLMES, information which is gathered in the course of counter-terrorism investigations is kept on a database, known as the National Special Branch Intelligence System, which is not linked to the Police National Database. As before, access to that information is confined to those directly involved in the investigation of this type of offending. Nevertheless, we found that the sharing of information

[48] We understand that there are no more recent figures available.

[49] Major Incident Room Standardised Administrative Procedures (MIRSAP), ACPO and Centrex, 2005, p37 para 1.15.1.

pertaining particularly to children and vulnerable adults was considered and appropriate action taken to make information more widely available in appropriate circumstances. This process forms part of continuing reviews of wider threat assessments in respect of counter-terrorism.

Professional standards department databases

Every police force has a professional standards department which investigates allegations of misconduct which are levelled against police officers in that force. Clearly, those who investigate these matters will gather information about the allegation and the suspect. Such information is generally kept on two separate databases: one relating to information and allegations of corruption, and the other relating to misconduct or other complaints. As before, these databases are not linked to the Police National Database.

Given these discrete information systems, it is clear that making an enquiry of the Police National Database alone may not be sufficient to provide a comprehensive picture of the police service's overall knowledge of any particular individual. Unless a decision is taken to include appropriate information from specialist departments as set out on the APP on information management[50], an officer who makes an enquiry of the Police National Database may be given only a partial view of what may be known about an individual by the police service as a whole.

Work is ongoing which will enable specialist police PND users to load their information into a secure restricted area of the PND known as a "dark group". This will permit the sharing and access to information between identified specialist PND users. At the time of writing this report, an implementation date for this service had not been established.

[50] *Authorised Professional Practice on information management, Common process for managing police information, Common process at force level, Recording,* College of Policing, 2013, para 1. Available at www.app.college.police.uk/app-content/information-management/management-of-police-information/common-process/#common-process-at-force-level

People and structures supporting information management

The APP on information management provides that:

> "Each chief constable is required to devise an information management strategy which sets out the principles of information management within a force. Amongst other matters, the strategy must set out:
>
> - who is responsible for police information held within the force;
> - the purpose for collecting and holding information;
> - which processes ensure that police information is audited for accuracy and relevance to the policing purpose;
> - the controls that are applied to ensure the integrity and security of police information held by the force;
> - arrangements for receiving records and monitoring record keeping; and
> - how the force complies with national and local security policy and standards." [51]

By setting out these matters in their information management strategy, each chief constable is able to demonstrate to the public that all information is being properly managed, retained and secured.

The guidance is also clear that there must be “key roles to support effective information management”. It also states that the chief officer:

- "has overall responsibility for a force's compliance with Home Office (2005) Code of Practice on the Management of Police Information;
- owns the IMS [information management strategy] and has responsibility for ensuring that force policies and processes comply with national guidance;
- may wish to appoint someone to oversee all information held by the force..." [52]

[51] *Authorised Professional Practice on information management, Common process for managing police information, Common process at force level, Information management strategy,* College of Policing, 2013, para 5. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/common-process/#information-management-strategy

[52] *Ibid,* para 6.

Findings

Information management strategy

The self-assessment survey of their information management practices carried out by all 43 forces in England and Wales in 2013 indicated that 36 forces have information management strategies in place. While this is a positive figure, we are concerned that, despite the unambiguous language used in the APP on information management, compliance was not universal: seven of the 43 police forces indicated that they did not have an information management strategy, despite the fact that it is clearly set out that such a strategy is required.

Of the 13 forces which we inspected we found that:

- one did not have an information management strategy at all;
- one had a document which was equivalent to such a strategy but its chief officers had abandoned its implementation because of technical difficulties, and an alternative strategy had not been formulated;
- a third force had introduced an information management strategy immediately prior to our inspection visit;
- five forces had not reviewed their information management strategies, and consequently they were not current; and
- three forces had not reviewed their information management processes that they set out in 2010.

Given the clarity of the requirement, those forces should develop their strategies quickly and implement them effectively.

Chief officers have constructed and implemented their information management strategies as they see fit. However, differences in approach across the police service as a whole mean that benefits that should come with all forces complying with the APP on information management are not realised.

HMIC found that each of the 13 forces we visited during our fieldwork had different information management operating models, even though they intended to achieve the same information management outcome. Only three of the forces we inspected had a policy that was closely aligned to the APP on information management and former editions of the national guidance. This is an unsustainable position if forces are to make the best use of information that is available to them and to protect the public from harm.

Responsibility for information management

In their responses to the national self-assessment survey, 40 (out of 43) police forces stated that they have appointed a chief officer with responsibility for the management of information in the force area. The same number of forces indicated that they had a records management policy or procedural guidance in place. A total of 36 forces have appointed a chief officer with specific responsibility for implementing the APP on information management and former editions of the national guidance that was issued in 2010.

Below the rank of chief officer, 29 forces stated they had a dedicated information management team to discharge expectations set out in the APP on information management and former editions of the national guidance; 30 forces stated that they had a records manager; 40 forces had a data protection officer; and 40 forces had an officer appointed to lead for the force on freedom of information requests.

Training, audit and performance management

HMIC was pleased to note that 38 forces stated that they have undertaken training in their forces regarding the APP on information management.

However, only 21 forces require local managers to conduct regular quality assured audits on the information that is held in their forces as required by the APP on information management;[53] and only 13 forces stated that they have performance indicators in place to measure the quality of their records management arrangements.

The vast majority of chief officers have taken steps to ensure that their forces have appointed chief information officer leads. These are officers who are responsible for specific areas of managing information, such as data protection, and policy statements which set out the forces' approaches.

These are all positive signs that some progress has been made.

However, we still have concerns about the practical day-to-day management of information. The absence of quality assurance audits in nearly half of the 43 forces and no performance management indicators in two-thirds of forces indicates that not enough attention is being paid to identifying how well the national guidance and local policies are being implemented and followed.

The familiar adage of "what gets measured gets done" applies to the forces here: when performance is monitored and measured, it is more likely that the required

[53] *Authorised Professional Practice on information management, Common process for managing police information, Retention, review and disposal, Audit and supervision of the review process,* College of Policing 2013, para 2.6. www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#audit-and-supervision-of-the-review-process

activity is undertaken and that improvements occur. When little or no attention is paid to finding out whether a force is complying with a policy, there is less incentive to reach a required standard.

Those forces which do not take that extra step and monitor the extent to which their officers comply with the national guidance and local policies should take immediate steps to ensure that their failure is corrected. They should emphasise the critical importance of sound and consistent information management policies and procedures, and the material risks to the public, and to police efficiency and effectiveness, when such policies and procedures are not soundly established and implemented.

Recommendation 3

> By 30 November 2015, chief constables should carry out systematic audits in their forces to identify the extent to which locally-adopted practices and procedures conform to the APP on information management.

Collection and recording of information

This section of the APP on information management reminds police officers that all police information must be accurate, adequate, relevant and timely.

The majority of information the police service receives is about people. As such, there are legal requirements on the police service to treat that information in a particular way. These are set out in the Data Protection Act 1998 and form the cornerstone of how any person or agency, including the police service, must deal with personal information.

The eight principles in the Data Protection Act 1998 are so important that we set them out in full here:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
    - at least one of the conditions in Schedule 2 is met, and
    - in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.54

[54] Part 1, Schedule 1, Data Protection Act 1998.

9. For the purpose of the first principle, the most relevant conditions with regard to the police service in Schedules 2 and 3 are the administration of justice55 and prospective legal proceedings.56

10. As the common process section of the APP on information management makes explicit, the Data Protection Act 1998 places a legal obligation on the chief officer, as data controller, to comply with the data protection principles, subject to exemptions, in relation to all personal information controlled by the force.

Findings

Standards for inputting or recording information about individuals

Against the clear requirements of Principle 4 of the Data Protection Act, we were concerned to note that only 30 police forces nationally have documented standards set out for inputting or recording of information about individuals. We consider that such standards are the first essential step in ensuring that all officers conform to data quality principles.[57]

Avoiding duplication of information

The self-assessment survey of the 43 forces in England and Wales that was carried out by the College of Policing indicated that only 32 forces have processes in place to manage duplicate or potentially duplicate records. This suggests that there a substantial amount of information kept on police databases that may be replicated elsewhere. This in turn means that the ability of officers to search databases efficiently may be impeded or frustrated because the search has to be undertaken of a greater number of records than need be the case.

Linking and referencing information

We were pleased to find that 35 police forces nationally do make the necessary links between new and existing information, and assess any new piece of information in the light of what is already known about the individual it concerns.

However, the national self-assessment survey on how forces link or reference information indicated that:

---

[55] Paragraph 5(a), Schedule 2, Data Protection Act 1998.

[56] Paragraph 6(a), Schedule 3, Data Protection Act 1998.

[57] *Authorised Professional Practice on Information Management, Collection and recording, Data quality principles,* College of Policing, 2013, para 3.3.1.2. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/collection-and-recording/#data-quality-principles

- two forces do not link or reference information on crime-recording;
- two forces do not do this in cases of child abuse or domestic violence;
- three forces do not do this in cases that involve public protection;
- seven forces do not do this in cases of missing persons;
- six forces do not do this with custody records; and
- one force does not do this with intelligence information.

Even in forces which do make the appropriate links, we found that the position was patchy, as there was no overall consistency or uniformity of approach.

(See further information on 'Uploading information to the Police National Database' on page 43.)

Linked databases[58]

We found that 5 forces out of the 13 which we visited were not able to reference all the information that was held about a named individual without having to search a number of separate computer systems. The results of the national self-assessment survey indicate that this is the position in ten police forces in England and Wales. This prevents efficiency and effectiveness, and these obstacles should be removed as soon as reasonably practicable.

Recommendation 4

> By November 2015, chief constables should ensure that adequate local information management processes are in place to consider all available information in an efficient and systematic way so that the continuing levels of risk that individuals pose to communities are properly assessed and, where necessary, information is recategorised and linked.

[58] See also the section on use of databases on page 25.

Evaluation of information

The process of evaluating information is critical. It is essential to have a consistent approach so that all forces are able to rely on the evaluation of the information by their colleagues.

All the information that the police service receives therefore must be evaluated in a way that the APP on information management states should be "appropriate to the policing purpose for which it was collected and recorded". This is to determine its provenance, accuracy and relevance to a policing purpose, and what action, if any, should be taken as a result of that information.

The initial assessment separates information from intelligence. The initial decision to treat information as possible intelligence is made by the police officer or member of police staff who receives it, either alone or with his line manager.

The guidance then sets out how the information which is treated as intelligence should be handled. In order to evaluate its importance in a consistent manner, the police service has established a process (called 5x5x5) which is designed to identify the level of risk and other factors attached to intelligence records.[59]

The guidance goes on to state that all information should be placed into one of four categories. These are set out in a different part of the guidance but they should be familiar to those who evaluate information:

- "Group 1 contains information about an individual that centres on the need for public protection. Information in group 1 is retained until the subject has reached 100 years of age.
- Group 2 contains information about an individual that centres on criminal offences outside those that trigger a group 1 classification but relate to sexual, violent or serious offences. Such information should be reviewed every ten years.

[59] This process was introduced under the National Intelligence Model. See *Introduction to intelligence-led policing*, produced on behalf of the Association of Chief Police Officers by the National Centre for Policing Excellence, 2007. It evaluates the source, the validity of the data and the handling sensitivity of a piece of information. Each category has five possible gradings and hence the system is universally known within the police service as 5x5x5. The five gradings for the source category range from "always reliable" to "untested source"; the five gradings for the data validity category range from "known to be true without reservation" to "suspected to be false"; and the gradings for the handling category range from "default: permits dissemination within the UK police service and other law enforcement agencies" to "permits dissemination but receiving agency to observe conditions as specified". In August 2012, changes were approved to handling category 4 to allow general sharing of that information type within the whole police service. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/evaluation/#5x5x5

- Group 3 contains information about those who are convicted, acquitted, charged, arrested, questioned or implicated in criminal behaviour which does not fall with groups 1 or 2. Such information must be retained for six years.[60]
- Group 4 contains information on undetected crime, missing persons and victims and witnesses".

Findings

Generally, police forces place the onus on the officer or member of police staff who initially receives the information to create a record and to apply the correct grading using the 5x5x5 grading system. That officer is often best placed to assess the level of risk which should be attached to the information, its sensitivity, and whether immediate action needs to be taken.

We were pleased to find that in all the forces we visited during our inspection, the initial officer's assessment was reviewed by a colleague who had been trained in grading intelligence. This gave us greater confidence in the quality of the decision regarding the grading of the information.

Categorising data

It is essential that the police service properly categorises the information it receives and does so in a timely manner. These categories are a good starting point in bringing similar types of information together, thereby allowing officers to narrow the amount of information which may have to be searched.

We were disappointed, therefore, to find that not all forces assessed were using the four categories identified in the guidance to group their information. Indeed, even in those forces which were, we found inconsistencies of approach in that the groupings were applied only in respect of certain types of information. This was the position in every force that we visited as part of our inspection.

Overall, 30 forces nationally do not comprehensively apply the groupings identified in the APP on information management. Even on the basis of the national self-assessment survey, this gives cause for concern.

Indexing

In eight of the forces we visited, relevant databases were searched to see whether there was any other information known about the individual who was the subject of the new piece of information, before that new piece of information was formally graded. Related records were then brought together and connections made. This

[60] Records within this group do not necessarily have to be reviewed and a force may opt to use a system of time-based, automatic disposal of information in this group, providing it satisfies the criteria laid down in the guidance.

process is known as indexing. Indexing ensures that records are searched and linked appropriately. It also enables previous information about the individual to be brought into the assessment of the new piece of information.

We found that the extent to which information was indexed, and the capacity to undertake this exercise, varied between and within forces. Additionally, we found that, in nine forces inspected, there was a backlog of information waiting to be indexed.

While information took its turn in the queue, we found that the new piece of information – which may have merited being shared with others through the Police National Database – was simply held at force level to await full evaluation.

This means that others who might search the PND would not be able to locate the new piece of information until that process has been completed at a local level. This defeats the purpose of the PND and increases the risk that relevant information is not shared, and public safety is compromised.

Not all the information which the forces receive can be indexed immediately. Four forces we inspected prioritised the indexing of more serious pieces of information, for example, by identifying them through use of key words (such as sexual assault, child abuse or vulnerable adults) that appear within the relevant record.

The adoption of a key word search enables forces to overcome the dangers of a backlog of data to process. It permits staff to prioritise the records of individuals who pose the greatest risk to our communities.

Recommendation 5

> By November 2015, chief constables should ensure that their local information management processes adequately identify and prioritise the records of those who pose the greatest risk, in order that they are properly monitored, and appropriate, timely action is taken.

Management of information (common process)

Once the information is evaluated, it has to be managed effectively. The APP on information management states that it should be in a format that is accessible and easy to use, whether it is an electronic, photographic or paper record.

Managing the information which they receive is essential for all police forces. As the APP on information management states*:*

> "[t]he integrity of police information relies on the information being trusted, acceptable, useable and available. It should be in a format that is acceptable and easy to use, whether it is electronic, photographic or paper record."[61]

It also states in mandatory language that:

> "[a]t force level the following is required:
>
> - processes to enable information to be linked and composite records to be maintained;
> - effective management of police records;
> - a central oversight of all information held within the organisation;
> - an information management strategy;
> - consistent processes to manage information as a corporate resource;
> - one business area to link to a record held within another business area. Processes should be shared where necessary."

The level and areas of compliance which the APP on information management specifies are clear. Effective management of information is essential if the police service is to make best use of everything that is known collectively.

If there were still any room for doubt about why this is required, the APP on information management dispels it in simple and clear language*:*

[61] *Authorised Professional Practice on information management – Common process for managing police information*, *Management of police records*, College of Policing, 2013, para 2. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/common-process/#management-of-police-records

> "The purpose of records management is to ensure that police information is documented and maintained in such a way that its evidential weight and integrity is not compromised over time. To achieve this, records need to be managed throughout their lifecycle, from creation through to disposal. This process requires records to be audited and maintained so that they remain a useful tool for policing purposes."

Findings

Reassessing and recategorising data

A flexible approach and a willingness to reconsider the importance of all pieces of information are essential if the police service is going to maintain an accurate and up-to-date assessment of the risk that any individual poses to the public at large.

As we have stated, it is also vital to consider the appropriateness of the group into which a piece of information is placed in the context of any further information relating to the same individual that comes to light. Indeed, this is a vital part of information assessment and enables a comprehensive picture of offending or suspicion to be formed. It is also part of Principle 3 of the Data Protection Act principles, namely that personal data "shall be adequate…" and Principle 4 that it "shall be ... kept up to date".62

Therefore, it is concerning to note that ten forces we inspected do not adjust the original classification of a piece of information in the light of any new information.

However, in four forces we inspected, we found a dedicated information management team whose practice was closely aligned to the principles set out in the guidance. They used an integrated information technology infrastructure which ensured that the most efficient use was made of the system's storage and search capabilities.

Typically, in those forces which adopted this approach, we found that the dedicated team was responsible for reviewing records and assessing the level of risk that any individual posed as a result of the information received. The team was able to adjust the categorisation of information in the light of any emerging new fact and, in turn, this informed those who took decisions about the need for any investigation into the individual.

In other forces subject to our inspection, there was a more fragmented approach with decisions to review cases taken at a more local level and, often, without reference to the rest of the information that was held about the individual.

[62] Paragraphs 3 and 4, Schedule 1, Data Protection Act 1998.

This latter approach engenders a greater degree of inconsistency, when the critical key for the police service as a whole is that officers within forces should be able to have confidence in the way in which their colleagues manage the information.

In those forces which did not fully adopt the national guidance, we expected to find reasoned policy decisions which were recorded to explain the local circumstances that demanded a different approach to be adopted. We found decisions to depart from the guidance recorded in only three of the forces we inspected.

Oversight and audit of the information management strategy

This theme of a lack of recorded decision-making continued when we considered the APP on information management requirement of independent oversight and auditing of the information management strategy at a force level.

We found limited evidence that such arrangements were in place in 11 of the forces which we visited. This suggests to us that those forces would not be able to provide any meaningful assurance that their teams were complying with even the local processes that had been adopted. This lack of oversight is a material gap in force arrangements.

Recommendation 6

> By 30 November 2015, chief constables should put in place arrangements to scrutinise audits of compliance with the APP on information management through the force information management governance structure. This should include measures to ensure that categorisation of records are regularly adjusted.

Sharing information

The APP on information management describes information-sharing as: "the processing of information either on a one-off or an ongoing basis between partners for the purpose of achieving a common aim." [63]

Clearly, with the volume of information which the police service acquires, it is important for every member of the public who may be affected by that information to be reassured that it is disclosed to others only in a controlled and uniform way, so that his privacy is not compromised inappropriately.

The ability to share information in a form that has the confidence of each party as to its integrity, accuracy and relevance is paramount for the police service. The days when would-be offenders stay in a single location and are "known to the police" are gone; those who wish to commit crime have the means, technology and know-how to do so without reference to artificial geographical boundaries. It is incumbent on the police service to ensure that the means by which it shares information between the 43 forces in England and Wales keeps up to speed with the ability of the offender to move from place to place.

Although our inspection did not consider the guidance on procedures to be followed when sharing information with other organisations, for the sake of completeness we mention here that the APP on information management sets out the procedures to be followed when sharing information between partner agencies.

However, in keeping with our approach that restricted our inspection to the issues arising out of HMIC's report into Savile, [64] we did not consider the extent to which individual forces share information with partner agencies outside the police service. We focused, instead, on arrangements that are in place which enable information to be accessed and shared between forces.

[63] *Authorised Professional Practice on information management, Sharing police information*, College of Policing, 2013, para 1. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/sharing/

[64] *Mistakes Were Made" - HMIC's review into allegations and intelligence material concerning Jimmy Savile between 1964 and 2012,* HMIC, March 2013. Available from www.justiceinspectorates.gov.uk/hmic/media/review-into-allegations-and-intelligence-material-concerning-jimmy-savile.pdf

Findings

Uploading information to the Police National Database

As we have said, the comprehensiveness and usefulness of a database is determined by the quality and completeness of the information that is uploaded onto it. If information is not uploaded onto the database at a force level, the value of the database as a repository of held information about an individual is diminished.

As we set out in ‘Use of databases’ on page 25, all police forces should ensure that information relating to the five core business areas of child abuse, domestic violence, custody, crime and intelligence are entered into local databases and that it is then uploaded onto the Police National Database.

We were pleased to find from the national self-assessment of forces that the vast majority of police forces do make sure that information is transferred to the Police National Database in a thorough way. However, if that database is to serve its purpose in the most effective way possible, it is essential that every force includes all its relevant information. An analysis of the national self-assessment survey of 43 forces in England and Wales shows that:

- two forces do not include records of recorded crime onto the database;
- four forces do not do this with custody records; and
- two forces do not do this with intelligence reports.

All of the 13 forces that we visited confirmed that their local procedures enable all relevant information to be transferred to the PND, but in practice this was done to varying degrees. Two forces were not able to provide data in respect of all five business areas: one was not providing data concerning custody; the other was not providing data concerning child abuse or domestic violence. Technical difficulties were cited as the reason why this was the case. These are serious omissions, but we are pleased to note that both forces are taking steps to correct these problems, and we will continue to monitor their progress.

(See further information on 'Next Steps’ on page 62.)

Retention, review and disposal of information

These final sections of the APP on information management focus on the way in which the police handle the information that they have acquired. Appropriately retaining information relating to an individual or suspected criminal activity is essential for the police service to develop and undertake investigations based on the National Intelligence Model of policing.[65]

However, retaining every piece of information which the police service receives without considering the need to do so is both unlawful and impractical. This is why the groupings set out in the APP on information management were created. They are there to help the police service band information into certain categories to maintain its database of knowledge.

The value, the risk associated with the piece of information and therefore the importance of individual pieces of information ebb and flow as time passes. It is simply impracticable for the police service collectively to retain every piece of information on the off-chance that on a date unspecified in the future, its value may resurface.

As the APP on information management states:

> "the review of police information is central to risk-based decision making [sic] and public protection. Records must be regularly reviewed to ensure that they remain necessary for a policing purpose, and are adequate and up to date."

To achieve a measure of consistency within and between forces, national retention assessment criteria have been established.[66]

In order to give effect to the requirements relevant to each group of information, police forces are required to hold scheduled reviews (except where automatic disposal is permissible under the guidance) so that an assessment of the risk of harm which the subject of the information under review may continue to pose can be made. Depending on the result of that review, a decision should be taken to retain or dispose of the information held about the subject.

---

[65] *Code of Practice – National Intelligence Model*, National Centre for Policing Excellence, 2005, made under sections 39 and 39A, Police Act 1996, and sections 28, 28A, 73 and 73A, Police Act 1997.

[66] *Authorised Professional Practice on information management, Retention, review and disposal, NRAC questions,* College of Policing, 2013, para 1.3.1. NRAC criteria: (i) evidence of capacity to inflict serious harm; (ii) concerns in relation to children or vulnerable adults; (iii) behaviour involving a breach of trust; (iv) evidence of established links or associations which might increase risk of harm; (v) evidence of substance misuse; (vi) concerns about individual's mental state. Available at www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#nrac-questions

Knowing what happens to individual pieces of information is essential if the police service is to apply the guidance properly and consistently. Therefore, there are requirements placed on those who oversee the management of information and intelligence to keep records of all triggered, scheduled and exception reviews of police records, regardless of whether they result in any charge.[67]

In addition, arrangements are required to be in place to inspect a sample of records held by the force about an individual so that there may be an independent assessment of the extent to which the force is complying with the guidance.

Findings

Retention

During our inspection, we found evidence that the guidance on the retention of information was not being uniformly and comprehensively applied. An analysis of the national self-assessment survey of 43 forces in England and Wales shows that:

- 35 forces retain group 1 information until the suspect reaches 100 years of age as required;
- 16 forces retain group 2 information for a 10-year period as required; and
- 17 forces retain group 3 information for a 6-year period as required.

This does not necessarily mean that other forces are disposing of their records ahead of the periods specified; they may be retaining records for longer than the guidance specifies. In respect of the information on serious specified, yet undetected crime, which is meant to be retained for 100 years, 37 forces indicated an intention to comply with the national guidance.

Compliance with other requirements in the national guidance concerning specific types of information, for example, about missing persons or victims and witnesses, varied between 42 forces and 37 forces respectively.

The national self-assessment survey indicated that, when making the decision whether to retain records about an individual, 23 forces do not take into consideration any information about the person that comes from outside the force.

This is of especially acute concern, given the extent to which individuals can quickly travel the length and breadth of the country, and abroad. Assessing information about an individual which is based on an artificial dividing line of a police force

[67] *Authorised Professional Practice on information management, Retention, review and disposal*, *Key roles in the review of information*, College of Policing, 2013, para 2.7. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#key-roles-in-the-review-of-information

boundary necessarily carries risks of compromising a full understanding of the real potential of that individual to commit crime.

A substantial majority of police forces comply with the national guidance in this area. However, the effectiveness of the Police National Database is a function of the quality – including timeliness – and comprehensive nature of the information it contains. If information is wrongly or prematurely deleted, it could compromise an investigation. Failures by police forces in the respects stated above have the potential to diminish materially that effectiveness. National decisions have been taken regarding the length of time which certain categories of information should be retained. It is clear that not all forces are conforming to that national guidance. Action must be taken to improve compliance.

Review

The guidance for the review process contains the appropriate procedures for making decisions on whether or not to retain information. Any record relating to a person is likely to go through three different reviews: an initial review where the information about him is evaluated; a scheduled review; and a triggered review.

Initial review

The initial review occurs when the information about the individual is put with any other information which is held about that person, and their composite value is assessed. The purpose of this review is to assess the risk that the individual poses based on all that is known about him, and accurately to categorise the information into one of the four groupings set out in the APP on information management.[68] The initial review enables the police to decide the way in which the information should be treated, subject to any reconsideration if there is further information that is acquired later.

We found that 10 of the 13 forces which we visited during our inspection were not undertaking initial reviews. Also, the national self-assessment survey indicates that as many as 30 police forces in England and Wales were not undertaking initial reviews. We understand that a full and timely information management review may not be reasonably practical in every case; for example, it would be unlawful to delay the release from custody of a detained person simply for the purpose of aggregating records known about them. However, a minimum set of checks and verifications could and should be undertaken.

The importance of carrying out a full review of aggregated information is of course greater in more serious cases, such as those involving children and vulnerable

[68] *Authorised Professional Practice on management of police information*, *Retention, review and disposal, Review schedule,* College of Policing, 2013, para 2.3.5. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#review-schedule

adults. The police should ensure that, if full compliance in every case is not to be mandatory, consideration should be given to the application of a principle and practice of proportionality. That is, of course, a matter for the College of Policing in its revision of the APP.

Recommendation 7

> By 30 November 2015, the College of Policing should amend its APP on information management so as to specify the minimum information management requirements for initial reviews in relation to the retention and disposal of information.

Scheduled review

A scheduled review is a reassessment of retained information for the purpose of determining whether or not it should continue to be retained. It takes place, as the name implies, at a point in time which is determined in advance, under the APP on information management. It comes, of course, after an initial review. As explained, it is at the initial review stage that the information in question is placed in one of the four specified categories. It is also an important way in which the police service is able to demonstrate its compliance with the case law in relation to the lawfulness of the holding of personal information about an individual.[69]

At the scheduled time, those reviewing the information should conduct a further assessment of the risk of harm which the individual poses. If that individual meets any of the criteria which are set out in the National Retention Assessment Criteria[70], the information should be retained and a further review date determined for another scheduled review.[71]

The results of the national survey and the findings from HMIC's inspection of 13 forces do not paint a convincing picture of compliance.

Only 18 forces stated that they review group 1 information every 10 years, as required in the guidance; 16 forces indicated that they reviewed group 2 information

---

[69] See, for example, *R (on the application of RMC and FJ) v Commissioner of Police of the Metropolis and Secretary of State for the Home Department and Liberty and Equality and Human Rights Commission* [2012] EWHC 1681 (Admin).

[70] Assessment criteria to assist in determining risk associated with the information content of a record. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#national-retention-assessment-criteria

[71] *Authorised Professional Practice management of police information, Retention, review and disposal*, *Scheduled reviews*, College of Policing, 2013, para 2.3. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#scheduled-reviews

every 10 years; and only 10 forces indicated that they had decided to deal with group 3 information by automatic disposal at the end of the 6-year period.

Overall, only 15 forces stated that they conducted scheduled reviews in compliance with the national guidance set out in the APP on information management.

Six forces which we visited indicated that they do not use the National Retention Assessment Criteria to reconsider the original classification of an item of information – in addition these forces did not provide a justification for decisions to retain information for a further period.

Recommendation 8

> Immediately, chief constables should make sure that their force information records are reviewed at the end of the review period set for each information grouping, and records created when decisions are made to retain information beyond the applicable period of retention.

Of further concern is the fact that the self-assessment survey of 43 forces nationally indicated that only 20 forces monitor the extent to which they comply with the applicable guidance.

This suggests that the majority of police forces do not know what their current level of compliance is in relation to the national guidance on reviews of information they hold. This is not acceptable and practice needs to change.

Triggered review

The force should carry out a triggered review whenever further information is submitted or obtained on a known individual.[72] This is particularly important when considering risks to children or vulnerable adults. A triggered review should be conducted in relation to all the information which the police hold on the individual concerned.

Triggered reviews are particularly important because they enable the police to consider the totality of the information they hold about an individual, based upon any new piece of information which they receive. This is the means by which seemingly innocuous pieces of information can be added to the mix of data already acquired about an individual, and a more comprehensive picture can be painted of that person's conduct. It is the start of identifying whether there are any more sinister trends based on the aggregation of information known about the individual.

[72] *Authorised Professional Practice management of police information, Retention, review and disposal*, *Triggered reviews*, College of Policing, 2013, para 2.2. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#triggered-reviews

A simple example explains the value of a triggered review: a single, one-off piece of information about an individual which discloses that he has been seen waiting outside school gates one day a week may seem innocent; but coupled with four separate pieces of information that indicate that the individual has been seen outside the gates of four other schools, once a day, on the other days of the week, builds a picture which suggests that the individual should be more closely monitored. This is the benefit which triggered reviews can bring to understanding the risk that an individual may pose to the community.

Five of the forces which we visited during our inspection were not undertaking triggered reviews. Of the eight forces that were, most were reviewing intelligence only, rather than all sources of information.

Overall, 30 forces stated in the national self-assessment survey that they conduct triggered reviews. These triggered reviews are an important tool in the assessment of the levels of risk in individual information records. Put together, they allow behavioural patterns to be identified more quickly. This allows for protective police interventions at an earlier stage. We consider this to be an essential process in risk management and the protection of the public. It is disappointing that not all forces have adopted this requirement.

Exception reviews

The purpose of review is to require a decision to be made whether a record should be disposed of or be retained. In respect of information that is identified as belonging to group 3 under the APP on information management, forces are able to operate an automated system for disposal based simply on the length of time for which the record has been held (see page 36). This is a practical way forward, given the volume of information that any one force retains in this grouping.

However, forces are required to highlight a person's record for an exception review if that person's behaviour suggests that they may pose a high risk of harm to others. Such a review takes the place of, and overrides, an automated disposal option.

Again, an example explains how this process should work. A person's record may disclose a conviction for theft. Of itself, that information might be placed in group 3 under the APP on information management, and therefore should become liable for automated disposal after a given period of time. However, that information might merit being reviewed on an exception basis if it transpires that the theft was of female underwear and was committed for the purpose of sexual gratification, because of the risk that an individual who behaves in such a way and with that intent might pose to members of the community at large.

During our inspection, we found that eight forces were not operating an exception review process, and the national self-assessment survey indicated that 27 forces did not do so.

The risk of disposing of information that continues to be relevant is obvious.

'Clear periods'

The timeframes for reviews are 10 years in the case of groups 1 and 2 information, and 6 years in the case of group 3.

It is necessary to make it plain: these lengths of time refer to so-called 'clear periods' that is the length of time since a person last came to the attention of the police as an offender or suspected offender in respect of behaviour that might be considered a relevant risk factor.

The concept of clear periods is sufficiently sophisticated to take into account periods of inactivity by an individual because he has been in prison or is known to have been abroad. In these instances, the clear period may be recalibrated to take into account such periods of inactivity.

Eight forces which we visited during our inspection did not retain group 2 information for a clear period of 10 years, and 7 forces did not do so for 6 years in respect of class 3 information.

Once again, this introduces police-initiated risks into the management of up-to-date information. It cannot be right that a person is deemed not to be a risk when the reason for the absence of any recent information centres on the fact that the individual was abroad or in prison during the original clear period, thereby providing an alternative explanation for that person's seeming inactivity, other than a new-found adherence to the law.

This gap in the effective assessment of clear periods (in determining the risk an individual poses to the public) is a matter of concern and must be addressed.

Disposal

Once a piece of information has been reviewed, it should be disposed of if there is no legitimate reason to retain it. But it is essential that the decision to dispose of a piece of information is taken in accordance with the guidance in the APP on information management.

Information that falls into groups 1 and 2 of the guidance should not be disposed of, other than after a review. This means that an automated disposal system based on the fact that a piece of information has reached the end of its retention period is not acceptable.

In the national self-assessment, 4 police forces indicated that they use an automated system for disposal with regard to information in groups 1 and 2. In addition, 9 forces nationally were considering automated systems for disposal of group 1 information, and 11 were considering automated disposal of group 2 information in the future.

Twenty-nine forces nationally indicated that they permit disposal of information based on a decision by one individual which does not need to be approved by a line manager. Therefore, the risk of inappropriate decisions being taken without a proper procedure for checking these decisions is clear.

During our inspection, we found that Hampshire Constabulary had instigated a 'peer review' process, in which decisions concerning higher risk records were considered by at least two experienced staff. Deletion of the highest risk records could only be undertaken following approval of the information governance manager. This is an example of good practice and it is important that other forces consider a similar level of oversight so that they may be satisfied that the decisions they take are appropriate.

Review processes for records created before 2006

As far as the management of police information is concerned, 2006 was a watershed year, as it saw the introduction of the Guidance on the Management of Police Information following the making of the Code of Practice on the Management of Police Information 2005.

But of course, introducing a standard regime applicable across the 43 forces of England and Wales for information acquired after its introduction is one thing; deciding how to integrate the information which had been acquired before that date is entirely another.

From earliest times, the police have acquired and kept information about those people who are criminals, suspected criminals or who pose risks to our communities. Many of the individuals who are the subjects of that information have records that pre-date 2006 by a considerable period of time.

Dovetailing the two sets of information is essential if a comprehensive analysis of the individual's behaviour is to be undertaken in a meaningful way.

This is made all the more difficult because the way in which records were created before 2006 varied: some were held in an electronic format, while many others were written down on paper and filed in a variety of ways.

It is sometimes easy to forget the time before information technology enabled searches of millions of records to be undertaken by typing in a single word and pressing a single button. Providing a comprehensive overview of all the information held on an individual, when many of those records might be in paper form in one filing cabinet among many others, without a comprehensive index of contents, is effectively impossible without many hours of research.

We are concerned about the findings in the national survey that only 34 out of 43 forces ensure that their review processes take into account pre-2006 information.

In addition, the means by which this is done is time-consuming in those business areas which are relevant to this inspection. This is because only 21 forces have made non-electronic records electronically searchable in information on crime recording. The corresponding percentages in respect of the remaining 4 business areas which formed the core of our inspection are: 21 forces nationally have searchable electronic domestic violence information; 23 have searchable child abuse information; 19 have searchable intelligence information; and 20 have searchable custody information.

Without being able to search those records electronically, it is highly unlikely that a comprehensive picture of a person's history, especially pre-2006, can be obtained.

The position is better but by no means complete when pre-2006 electronic records are considered. Where this is the case, 36 forces have systems in place to search electronically with regard to crime recording; 35 forces with regard to records relating to domestic violence and child abuse; 34 forces with regard to custody records; and 36 forces with regard to intelligence information.

Management of sensitive information

Because of the classification given to some information during the investigations into Savile, we were keen to understand, in particular, how police forces deal with sensitive information. We focused on information acquired in major crime investigations; in the field of counter-terrorism; and as a result of enquires conducted in the professional standards departments of the 43 police forces in England and Wales.

Findings

National guidance

To meet the concerns which these specialised areas of police work raise, a project into how sensitive information is handled was established by the National Policing Improvement Agency in May 2006. This work aimed to establish how best the information generated in specialised areas of police work could be made available to those in non-specialist areas of policing.

The project resulted in guidance on how sensitive information should be managed, and it was published in December 2008 as a supplement to the Guidance on the Management of Police Information. This supplementary guidance was not formally incorporated into the second edition of the Guidance on the Management of Police Information which was published in 2010; neither has the supplementary guidance been incorporated into the APP on information management.

As a result, we found evidence that different practices are being followed in the 43 police forces in England and Wales with regard to the handling of sensitive information.

We were also concerned to note that only in four of the forces which we visited was there any force-wide policy setting out how sensitive information should be treated. Even in those four forces, we did not find any evidence to show that compliance with the policy was being monitored to ensure that it was being followed. The absence of consistent practice together with differences of approach in implementation results compromises the ability to manage information effectively.

Recommendation 9

> By 30 November 2015, the College of Policing should ensure that specific guidance about the handling and availability of sensitive information is included in the APP on information management, and by 30 June 2016, chief constables should ensure that the guidance set out concerning sensitive information is implemented.

Sharing sensitive information

As a result of the information which certain types of investigation acquire, it may be necessary to restrict access by others who are not directly connected to a specific investigation.

There is a clear tension here. Sensitive information acquired in such enquiries is exactly that: sensitive. It is right that such information should only be available to those who need it. However, there will also be occasions when sensitive information may be highly relevant in unrelated investigations, for example, in instances when the focus centres on a child who may need to be protected, or on a person who may be seen as vulnerable. When the focus is on a potential offender, the information may well be seen as sensitive; but when the lens is retrained to consider the matter from the potential victim's point of view, that which was sensitive may assume an overwhelming relevance to the issues as they affect the potential victim.

In order to strike a balance between what may be considered competing interests, the information management systems used to manage sensitive information are separate from those systems used to store non-sensitive information. This was the case in all the forces which we visited. And in all instances, the sensitive information was not automatically or directly supplied to the Police National Database. This allows decisions to be taken as to the suitability of sharing the information on a case-by-case basis before it is included in the Police National Database.

Given the fact that Savile was allowed to continue his pattern of sexual assault for so long, in part because sensitive information was not made available to forces in their later enquiries into his conduct, it is a matter of material concern to note that this position does not appear to have improved.

Forces should not lose sight of the fact that, for the reasons we have set out above, even sensitive information may need to be shared if the whole picture regarding dangerous offenders is to be made available to the rest of the police service. Forces should devise a means by which sensitive information is recognised, assessed and appropriately transferred onto the Police National Database which can then be searched by others, so that they may be made aware that sensitive information exists in respect of their person of interest.

Major crime investigations

Investigations under this heading use HOLMES to house the information which is acquired. This can often run into thousands of pieces of information, as the original net of enquiries may be cast widely. The following case study provides an example of the sort of enquiries in question, and the types of information that are obtained.

Case study

A number of attempts to abduct children in a small town were investigated by a Major Crime Investigation Unit. The investigation was recorded and managed on the Home Office Large Major Enquiry System.

The senior investigating officer's strategy was to focus on the original allegations, conduct witness video interviews with the children who made the allegations, and establish the facts.

After the interviews, it became apparent that there were two instances, involving two children, as opposed to the initially-reported five abduction attempts.

The children were able to provide a basic description of the offender and a decision was made to trace, interview and eliminate all registered sex offenders[73] within the locality who broadly matched the description provided by the children of a white, English-speaking male.

This is a common strategy in cases of this nature.

There was no forensic evidence.

A significant amount of research and development was undertaken by the investigation team. A great deal of information gathered centred on registered sex offenders who, although eliminated as suspects for this crime, remained as individuals who presented a risk to the public in a wider context. There would be a need for this information to be made more widely available within police information systems.

This example demonstrates the volume of information that may be obtained in major enquiries, not all of which will be relevant to the final outcome in the particular case in which it was acquired. The seemingly irrelevant information in this case might prove of help in other cases, and this is the very purpose of gathering and evaluating all the information that the police service acquires.

A simple example illustrates the point that is being made in this report: in the course of the enquiry carried out in the case study above, a registered sex offender may have been interviewed and he may have stated that he was in another town at the time in question – a fact that could be verified.

[73] Sections 80 and 81, Sexual Offences Act 2003 require details of those who commit certain sexual offences to be notified to the police. Those individuals who are subject to this requirement are commonly known as registered sex offenders.

That person may no longer be of interest in the enquiry in respect of which he was interviewed, but to officers in that second town who may be investigating an allegation of sexual assault on a child, the fact that that individual admitted to being present in their town may well be highly relevant. Without the means of ensuring that the information from HOLMES is made available to others, that potentially relevant piece of information might be lost.

The information on HOLMES is not automatically uploaded into the Police National Database. However, we found that two of the forces which we visited had developed the technical capability to make a record on HOLMES that was visible using the force's search facility. This enabled local force systems to be alerted to the presence of related information on HOLMES.

Merseyside Police is making substantial advances in this area. There, a senior investigator identifies suitable records for more widespread circulation. A process has been developed which allows those records to be transferred to an electronic data storage area which then is uploaded onto the Police National Database. As far as we are aware, this is the first force in England and Wales to have developed this. We welcome the Merseyside Police initiative but have concerns that the initiative is in isolation from other forces. There is a need to introduce a common standard and common approach to address this deficiency throughout England and Wales.

However, this does not address the concern that officers in the remaining 41 forces are still not able to do so.

Counter-terrorism

The police service's response to the threat of terrorism and domestic extremism is managed through a national network of dedicated police officers. Since about 2003, the National Special Branch Intelligence System has been used to manage the records which relate to enquiries into such matters.

Although the intelligence system is common to all the teams of investigators looking into these types of crime, individual counter-terrorism units are permitted to change and customise aspects of their databases if they so wish.

This has led to inconsistent and varied information-recording practices.

This weakness has been identified and work is underway to standardise the approach adopted both to the management of the information which the teams of investigators acquire, and the information technology systems which they use.

This is in advance of a replacement programme which will involve the introduction of a new National Common Intelligence Application. This application will enable appropriately authorised individuals to be given access to view the whole picture of counter-terrorism in the United Kingdom.

It will be supported by standard operating procedures and national standards of intelligence management. In this way, information will be entered and processed in a consistent manner and will no longer be varied according to the particular team of investigators which acquired it.

Part of the development of the application involves identifying ways and formal processes to make available, on a broader scale, intelligence that indicates a threat or risk to more general policing activities. This needs to be done in a way that continues to protect the highly sensitive information derived from counter-terrorism sources and the means by which any policing tactics secure information.

During our inspection, we found that forces have been investing time and resources into ensuring that the data contained in their National Special Branch Intelligence Systems is suitable to transfer onto the National Common Intelligence Application. This has involved ensuring that it is in a common format so that all the information, no matter its source, may be treated, read and stored in the same way.

We were pleased to note that, in the East Midlands region of police forces,[74] common standards and working practices have already been developed and implemented in anticipation of the national approach. They already have the benefit of being able to access and read all information relating to counter-terrorism within their regional forces' group. They are the first in the country to establish this capability.

Although specifically targeted towards meeting the terrorism threat, the teams of investigators do acquire information which is of value in other lines of investigative work. Although we did not find examples of specific policies or any audit trails regarding what should and did happen to such information, we found that officers in those teams were considering the wider picture and applying professional judgment in deciding how to make such information better available to their colleagues as part of their continuous risk-assessment processes.

Professional standards

Information acquired by the professional standards departments of the 43 police forces can generally be divided into information concerning allegations of misconduct and complaints, and information concerning allegations of corruption.

During our fieldwork, we found substantially different approaches were being taken by the professional standards departments to the sharing of the information which their officers acquired. We found two extremes and differing positions between the two. On one side, one force adopted a position not to share information with anyone else and retained that information indefinitely without review; on the other side,

[74] The East Midlands region of police forces comprises: Derbyshire Constabulary; Leicestershire Police; Lincolnshire Police; Northamptonshire Police; and Nottinghamshire Police.

another force regularly reviewed the information which it acquired in these circumstances and added markers to the intelligence systems to show that additional information of a sensitive nature was held elsewhere. Those markers were uploaded onto the Police National Database and, accordingly, officers investigating other matters were at least put on notice that further information was available which might have a bearing on their cases.

As we have explained, regular consideration of a piece of information's value is essential in order to follow up critical intelligence opportunities and to honour the principles of the Data Protection Act 1998. This applies as much to sensitive information as it does to other types of information. Indeed, there is provision for sensitive information to be reclassified to make it more widely available, as and when circumstances permit.

We specifically considered whether sensitive information had been reconsidered in this way. We found that, in eight of the forces that we inspected, there was no standard process for the review of information that had initially been marked in such a way as to prevent its availability to others in the police service. In some of those eight forces, we did identify instances where such reviews had taken place. However, they appear to have been undertaken inconsistently and only because of the individual professionalism of the officers concerned, rather than as a result of any force policy which required such reviews. This is of concern and should be a matter of force direction and policy.

Recommendation 10

> By 30 November 2015, the College of Policing should revise the current APP on information management and include a common review process in respect of sensitive information for adoption by all forces. This should include timescales for the review of sensitive information in order to ensure it remains appropriately categorised.

Conclusions

A cornerstone of effective police investigations is a full, evidence-based evaluation of the risk that an individual poses to the community. Such an evaluation cannot be achieved without understanding all the information which the police service as a whole has about any individual. And that understanding cannot be secured without effective systems in place to manage efficiently the information that the police service acquires every hour of every day, every day of the year, so that it is available in proper form to those who need it, when they need it.

Without effective and consistent management of this police information, potential offenders will not be stopped before harm is done; criminals will continue to offend; and law-abiding members of our community will become needless victims of preventable crimes.

There are sound legal reasons why the police service needs to adhere to a rigorous and approved set of processes for managing police information. The Data Protection Act 1998 and the developing case law on the extent to which personal information may properly be retained by the police service act as reminders of the need for sound and comprehensive information management processes. These must be fully complied with, properly recorded and rigorously overseen. Mistakes made by police forces because they have not taken steps to ensure compliance with law and practice are avoidable and must be rectified.

The Code of Practice on the Management of Police Information 2005, the APP on information management and former editions of the national guidance do not spell out the importance of achieving consistency in the application of management of information principles across all police forces. Inconsistencies can reduce opportunities to link information, losing the crime-fighting advantages of “joining the dots”.

In the light of case law and high-profile cases such as Jimmy Savile’s long period of sex offending, we are materially concerned about the extent to which the police service is responding fully to the responsibilities inherent in a changing environment, where speedy access to up-to-date and relevant information is essential.

How forces address their responsibilities on good management of police information remains a matter for individual chief constables. However, during our inspection we found that:

- There is insufficient review taking place of the information that forces hold. Without these reviews – and the means to demonstrate that they have taken place properly, or at all – the police service leaves itself vulnerable to challenge. The absence of sound and consistent reviews means that information might be destroyed when it should be kept, thus increasing the risk to public safety, which is a matter of serious concern.

- The volume of information acquired by the police means that not every piece of information can be evaluated and processed at the same time. The question then arises of how to identify those pieces of information which demand more immediate consideration than others. Clearly, the information which informs the police of a greater or more immediate risk to the public should be considered as soon as possible. We found that the extent to which information was reviewed, prioritised and indexed, and the capacity to undertake this exercise, varied between and within forces. However, four forces we inspected use a process based on key words.[75] We found that this approach appears to work well, and offers a sensible way forward when decisions have to be made about which piece of information to consider next.

- A significant strand of our inspection examined how sensitive information is handled, particularly when it is acquired and held as a result of specialist policing activities, such as major crime investigations; counter-terrorism investigations; and internal investigations of police staff for misconduct; corruption or other criminal offences. We found current deficiencies in the management and accessibility of sensitive information. It is important that forces develop better integration between the IT systems which host such information and the principal databases available to the police. If our findings are addressed, policing effectiveness is improved and the risks to the public associated with the current failure to share such information are reduced.

- There is a need, particularly with information that has been marked sensitive at one time, for the police to review it to see whether such a classification remains appropriate as time passes. It is concerning that this is not always done. Much more can and should be done to refresh the categorisation of information from when it is first received and assessed. The importance of information fluctuates with the passing of time and the police service must do significantly more to reflect that fact, particularly with regard to sensitive information such as that hosted in HOLMES.

[75] 'Key words' are a local force term to describe highlighting certain records to make them identifiable when searching for information, as described on page 35.

- Forces which maintained a central information management team were able better to adopt the principles of the APP on information management and former editions of the national guidance. This was especially the case when those teams had access to an integrated computer system where officers could reference and facilitate the assessment of all the information held on a named individual, without the need to search separate computer systems.

- Some forces had recognised the risks arising from the restricted availability of some information contained only in HOLMES. We applaud those forces which are developing the means to identify, isolate and transfer appropriate records on a case-by-case basis, so that they can be used to "build the picture" of intelligence at a local level. We would like to see this developed further. All forces, as soon as economically feasible, should take similar action to those forces to ensure information from HOLMES is handled in a consistent way, and in particular is made more widely available.

- The national self-assessment survey indicated that 30 forces conduct triggered reviews. These triggered reviews are an important tool in the assessment of the levels of risk in individual information records. Put together, they allow behavioural patterns to be identified more quickly. This allows for protective police interventions at an earlier stage. We consider this to be an essential process in risk management and the protection of the public. It is disappointing that not all forces have adopted this requirement.

It would be unrealistic for the police service to make categorical assurances that the risk posed by predatory offenders could be eradicated on the sole basis of improvements in the management of police information. Nevertheless, there is a real and pressing need for greater attention to be paid to the management of police information, so that greater consistency is achieved across all forces. It is not enough that some forces manage information better than others. The purpose of a national system is to ensure that, as far as possible, relevant information is available to the right person at the right time, no matter in what part of the country that piece of information was generated.

It may have been necessary initially to allow the exercise of local discretion to adjust management information practices to get the system up and running, particularly in the absence of a comprehensive IT solution. But in today's environment, local variations in practice carry real risks that the mistakes we identified in our report about police contact with Jimmy Savile could be repeated.

Greater rigour in the implementation of management information policies is required so that all forces are brought up to the standards of the best.

Next steps

From time to time we will monitor compliance with the APP on information management in order to encourage learning opportunities from good practice and scrutinising the weaknesses we have identified in this report.

As a first step, we will check the implementation of our recommendations in this report through HMIC's current monitoring procedures, and thereafter work with the College of Policing to design a focused inspection to determine what progress has been made.

Summary of recommendations

To the Home Office and the National Lead for Information Management Business Area

Recommendation 2

By May 2016, the Home Office and National Police Chiefs' Council's Information Management Business Area lead, should agree and implement common standards to be used by forces to identify and transfer information, no longer sensitive to an enquiry contained within HOLMES, to systems which are accessible and searchable by the police service generally.

To chief constables

Recommendation 1

By 30 November 2015, chief constables should ensure that a review is undertaken of the way in which their forces' information management policies and practice comply with the APP on information management so that they give effect to the national approach and minimise any divergence from that APP.

Recommendation 3

By 30 November 2015, chief constables should carry out systematic audits in their forces to identify the extent to which locally-adopted practices and procedures conform to the APP on information management.

Recommendation 4

By November 2015, chief constables should ensure that adequate local information management processes are in place to consider all available information in an efficient and systematic way so that the continuing levels of risk that individuals pose to communities are properly assessed and, where necessary, information is recategorised and linked.

Recommendation 5

By November 2015, chief constables should ensure that their local information management processes adequately identify and prioritise the records of those who pose the greatest risk, in order that they are properly monitored, and appropriate, timely action is taken.

Recommendation 6

By 30 November 2015, chief constables should put in place arrangements to scrutinise audits of compliance with the APP on information management through the force information management governance structure. This should include measures to ensure that categorisation of records are regularly adjusted.

Recommendation 8

Immediately, chief constables should make sure that their force information records are reviewed at the end of the review period set for each information grouping, and records created when decisions are made to retain information beyond the applicable period of retention.

To the College of Policing

Recommendation 7

By 30 November 2015, the College of Policing should amend its APP on information management so as to specify the minimum information management requirements for initial reviews in relation to the retention and disposal of information.

Recommendation 9

By 30 November 2015, the College of Policing should ensure that specific guidance about the handling and availability of sensitive information is included in the APP on information management, and by 30 June 2016, chief constables should ensure that the guidance set out concerning sensitive information, is implemented.

Recommendation 10

By 30 November 2015, the College of Policing should revise the current APP on information management and include a common review process in respect of sensitive information for adoption by all forces. This should include timescales for the review of sensitive information in order to ensure it remains appropriately categorised.

Annex A - Terms of reference

Purpose

This purpose of this inspection was to follow up on the findings from the Savile Review in 'Mistakes Were Made' and to discharge HMIC's responsibilities to monitor compliance with the Management of Police Information Code of Practice.

Background

The Bichard Inquiry, following the Soham murders, made recommendations to the police service in respect of managing information. In 2011, the Police National Database was first introduced to provide a national information sharing platform and develop police intelligence capability; a second release of the Police National Database was launched in 2012. Further releases of PND functionality have subsequently been introduced.

On 7 November 2012, HMIC was commissioned by the Home Secretary to review reports and allegations in respect of Jimmy Savile. This review extended in the event of discovering police failings to identify wider lessons learnt.

The HMIC Savile review report, published on 12 March 2013, identified significant issues with police information management in five forces including classification, restriction, provision and the sharing of intelligence in respect of six records relating to identifying paedophilic activity and sexual offences against children. This is despite some progress since the Bichard Inquiry and the advent of the Police National Database.

In addition, the Management of Police Information Code of Practice (July 2005), which forms the legal basis requiring forces to align to the Code's information management principles, also places an obligation on HMIC to ensure that effective and efficient processes are nationally adopted and remain in place.

> "1.3.1 HM Inspectors of Constabulary will monitor police forces' compliance with this Code, associated guidance, and standards "

There has never been a dedicated and specific HMIC inspection or review relating to information management.

Objectives

The objectives of the inspection activities were to establish:

- if force strategies, policies and procedures for information management adhere to the principles of the management of police information [and the Authorised Professional Practice] doctrine, and are proportionate to risk and fit for purpose;
- if information and intelligence are captured, recorded, evaluated, acted upon, audited and retained by the police (including safeguarding interventions) in an effective way;
- if the use of the Police National Database is effective and efficient;
- if HMIC can identify inspection criteria that can be introduced into other future inspections. (This would allow regular and frequent monitoring of information management in forces to discharge HMIC's legal obligation, without the need for further specific inspection activity).

Inspection approach

The four forces involved in the Savile review and two forces involved in the Bichard Inquiry were inspected. Independently, the national Information Management Business Area has commissioned the College of Policing to devise a national questionnaire which has been circulated to all forces. The responses have been collated to ascertain the current national information management picture, post-Savile. The findings from the questionnaire responses were shared with HMIC in order to avoid duplication and the need to ask similar questions. This formed the basis for the broad review of force capability and further forces were identified for inspection from the questionnaire analysis.

The inspection was executed in two phases:

- Phase 1 analysed responses from the national information management force questionnaire. There was a need to ask specific supplementary questions of forces concerning the management of sensitive information to address concerns identified within the Savile report. The questionnaires were collated and analysed to identify areas for targeted fieldwork.
- HMIC conducted a reality check in order to ensure the integrity of the national questionnaire responses and re-evaluation process.

- Phase 2 consisted of an inspection in 13 forces (including the core 6 Savile and Bichard forces) to provide empirical, quantitative and qualitative information regarding the specific areas that were identified and were in the Savile report. This identified the scale of the issues identified and built on the earlier Savile report.

As a result of the inspection, generic information management review criteria were identified for use in future HMIC inspections, thus discharging HMIC's responsibility as detailed in the Management of Police Information Code of Practice in perpetuity, and avoiding the need for further specific inspections on information management.

Methodology

HMIC wrote to all chief constables and police and crime commissioners introducing the inspection. The national information business area lead was already aware of the proposal and it was published in the HMIC business plan.

A programme board chaired by the SRO [Her Majesty's Inspector, Dru Sharpling] was set up to oversee the progress of the project.

Inspection activity in forces consisted of two distinct elements:

- Desktop review: this included an evaluation of the IMBA questionnaire response and a review of relevant policies and strategies to inform the fieldwork;
- Fieldwork: this involved interviews of relevant staff, and reality testing of the issues emerging from the Savile report.

Fieldwork examined:

- how information is recorded, reviewed, retained and deleted;
- the provision, quality and timeliness of data put into PND;
- the process for inclusion and handling of sensitive information;
- the ability of forces to automate or link police information and intelligence data.

The fieldwork consisted of interviews and focus groups with relevant staff and was conducted by a team of information management subject specialists.

An emerging findings debrief was offered to each force at the conclusion of fieldwork. For each force visited, HMIC provided a detailed feedback report to the chief officer and the police and crime commissioner.

In addition, HMIC committed to produce a national thematic report reflecting strengths and areas for improvement enabling all forces to improve the management of information. This report meets that commitment.

Annex B – Evolution of national guidance

The statutory Code of Practice and associated guidance

As we have set out, in 2005, the Home Secretary issued a Code of Practice on the Management of Police Information.[76] In 2006, the Central Police Training and Development Authority produced, on behalf of the Association of Chief Police Officers, Guidance on the Management of Police Information, which was published by the National Centre for Policing Excellence. This was revised in 2010 by the National Policing Improvement Agency resulting in the publication of a second edition.

That 2010 guidance has now been superseded by the Authorised Professional Practice on information management which was published in October 2013.[77] This is the body of guidance published by the College of Policing to provide the police service in England and Wales with policy and procedures to follow.

As it is relevant to our inspection, we set out below a brief summary of the guidance's evolution.

The 2006 and 2010 Guidance on the Management of Police Information put a framework in place to improve the way forces collect, record, evaluate, review and improve the quality of information. Its overarching objective was to contribute to enhanced public safety by improving the ability of the police service properly to manage and share operational information within a nationally consistent framework.

In December 2010, 34 of the 43 police forces in England and Wales stated that they had implemented the guidance; it was a self-declaration.[78]

The guidance recommended that forces should review their records from April 2006 and categorise them to ensure a consistent approach to information management across forces.

Although the guidance applied to all police information created after April 2006, mechanisms existed to deal with information that pre-dated its introduction. If a

---

[76] Code of Practice on the Management of Police Information issued under sections 39 and 39A, Police Act 1996 and sections 28, 28A, 73 and 73A of the Police Act 1997. Available from http://library.college.police.uk/docs/homeoffice/codeofpracticefinal12073.pdf

[77] *Authorised Professional Practice on information management,* College of Policing, October 2013. Available from www.app.college.police.uk/app-content/information-management

[78] Care should be taken with this figure. The 34 police forces stated that they had completed that which they intended to implement by way of the management of police information, which may or may not have been completely in alignment with the national guidance. As far as we are aware, there has not been any more recent assessment of the extent of compliance.

person came to police attention after that date, but about whom there was information from before April 2006, the guidance advised that a review should take place that encompassed all known previous related records, thereby ensuring historical (including paper) records formed part of an overall and comprehensive assessment of the individual.

One of the main reasons for the introduction of the guidance was to address this very issue and one of its principal objectives was to cause seemingly innocuous pieces of information to be gathered, collated and assessed in order to build a more comprehensive picture of what might be more sinister behaviour, offending or trends.

The guidance prioritised information according to risk; as a result, information which indicates children or vulnerable adults are at risk should receive particular attention.

The 2010 guidance has now been superseded but the basis of it forms the APP on information management.[79]

[79] *Authorised Professional Practice on information management*, College of Policing, 2013. Available from www.app.college.police.uk/app-content/information-management/management-of-police-information/ This is the body of guidance published by the College of Policing to provide the police service in England and Wales with policy and procedures to follow.