Policy & Procedure

Title: **Records Management Policy**	**URN ES 60 (formerly CDB 3015)**

Contents

Part One - Policy

Policy Summary

This policy covers the management of operational Policing information in line with the 2005 Code of Practice on the Management of Police Information (MoPI).

Aim

This document details practical guidance for the application of the force's Information Management Strategy.

The **Code of Ethics** published in 2014 by the College of Policing requires us all to do the right thing in the right way. It also recognises that the use of discretion in Policing is necessary but in using discretion, states that you should, "*take into account any relevant policing codes, guidance, policies and procedures into consideration.*"

Scope

This policy applies to all Humberside Police Staff. It also applies to members of other organisations who are authorised to record Humberside Police information, including members of partner organisations.

It is applicable to all information entered on police systems, primarily (though not exclusively) those feeding the Police National Database (PND):

Compliance

This Policy is intended to comply with the following legislation and guidance:

- Police and Criminal Evidence Act 1984
- Criminal Procedure and Investigations Act 1996
- Authorised Professional Practice - Information Management
- Data Protection Act 2018
- Freedom of Information Act 2000
- Authorised Professional Practice (APP)

- Human Rights Act 1998
- Part V of the Police Act 1997

Principles

This policy covers information for a policing purpose, as defined by the Authorised Professional Practice on Information Management, i.e.:

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

Related Guidelines

- Records Management - Disposal Schedule
- Review, Retention and Disposal Policy and Working Practice
- Information Management Strategy
- Information Sharing Policy
- Information Security Policy

Further Advice

Further advice on the contents of this policy may be obtained from:

- Records Manager

Part Two – Policy Procedure

Chapter One

1. Records Management

1.1 The term “record” refers to any written, electronic, digital, magnetic or paper based information including photographic and other optical media recorded for one or more of the purposes outlined above.

1.2 This policy does not presently explicitly cover the following records:

- Electronic mail;
- Electronic filing or storage systems (e.g. personal folders);

1.3 This policy does not presently cover the following areas, but is intended to do so in future revisions:

- Preservation of records (including backups of electronic records);
- Provisions for access to inactive/archived records;
- Business continuity plans for the maintenance of records.

2. Ownership of Data

2.1 The force’s information Management Strategy states that each business area will have a named owner of information.

2.2 The force’s Records Management Section has the authority to amend data on behalf of the information owners.

Chapter Two

3. Principles of Recording

3.1 There are a number of key principles which apply to the recording of police information regardless of the format and business area in which it is held.

- A record must have been created for a policing purpose.
- All records must comply with the data quality principles set out below.
- A record of police information is the start of an audit trail and must identify who completed the record, when it was completed and for what purpose.
- Before recording information checks must be made in other business areas to see whether the information is already held elsewhere to avoid unnecessary duplication.
- If information is recorded on an individual who is the subject of an existing record in another system, then the new record should reflect this.
- If it becomes apparent that the information being recorded is connected with other information then it must be appropriately linked.
- Police information should be recorded on a core system (see 5.2) as soon as practicable in accordance with the standards relating to the business area in which the information is held.
- Before recording police information consideration must be given to any sensitivities in recording it to ensure that it is given the appropriate Government Protective Marking Scheme (GPMS) marking.
- Every effort should be made to avoid unnecessary duplication of records.

4. Data Quality Principles

4.1 All Humberside Police information must conform to the following data quality principles:

- **Accurate** – care must be taken when recording information and, where appropriate, the source of the information must also be recorded. If there is any doubt over the authenticity of the information, clarification should be obtained from the source and marked with the appropriate 5x3x2 classification. Inaccurate information must be corrected as soon as possible. In ensuring accuracy it is important not to delete historic information that may be significant (such as details of previous addresses)

- **Adequate** – recorded information must be accurate and sufficient for the policing purpose in which it is processed. All recorded information must be easily understood by others.

- **Relevant** – information recorded must be relevant to the policing purpose. Opinions need to be clearly distinguished from fact and recorded in professional language.

- **Timely** – information must be promptly recorded into the relevant business area in accordance with agreed timescales.

- **Consistent** – all information must be collected and recorded in compliance with national and/or force standards. This standardisation of format and conventions allows for accurate searching and retrieval of information and its subsequent analysis and interpretation.

- **Complete** – all relevant information that is collected must be recorded into the appropriate designated fields of force electronic or paper systems. In order to make information more usable and identifiable there is a need to collect and record all the necessary and relevant data that can be ascertained at the time of collection or recording.

  A record cannot be classified as complete until **all** the relevant information that has been recorded is recorded into the appropriate designated fields.

5. How Police Information is recorded

5.1 Where there is a conflict between data recording standards, any national guidance takes precedence, followed by local standard operating procedures, followed by the generic guidance within the Records Management Policy. Any identified conflicts between standards must be reported to the Force Records Manager.

5.2 The force's Core Systems is CONNECT with legacy systems of: CIS4 (crime, intelligence and domestic violence), CATS (Child Protection Database), NSPIS Case and Custody and the National Firearms Licensing System (NFLMS).

5.3 Information recorded outside of these systems will not be available for operational decision making either internally (via the LYNX search tool) or externally (via the Police National Database – PND). Information recorded for a policing purpose should be recorded in, or transferred to, one of these core systems wherever practicable.

5.4 Guidance on managing non-core databases is detailed in Appendix 2.

6. Information Sharing

6.1 Information must only be shared in line with the force's Information Sharing Policy.

6.2 Where possible, Information Sharing Agreements (ISAs) should be set up to cover instances where information is regularly shared.

6.3 Decisions whether to share information outside of Information Sharing Agreements must be recorded in line with the guidance in the Information Sharing Policy, whether any information is shared or not.

Chapter Three

7. Person Records

7.1 For **all** person records, it is essential that as much information as possible is collected to establish or verify a person's identity. This approach acknowledges the legal requirement to process personal information appropriately as set out in the Data Protection Act (1998).

7.2 **The minimum for a definitive identification of a person is a full name and date of birth.**

7.3 If available, a PNCID or CRO must be used to confirm the identity of a person who is already recorded on a force system. The PNCID shall be used as the primary identifier for a person record.

7.4 Where an IT system contains discrete, searchable fields for names these **must** be used to record the details of any person named on that record.

8. Suspects

8.1 Suspect records are a subset of person records and so should be recorded to the same standards, particularly with regard to names being entered into appropriate fields where provided.

8.2 At any time in an investigation, a person can be classed as a "suspect" when there are reasonable grounds to suspect they have been involved in an offence or incident. Reasonable grounds do not have to be sufficient for arrest but should have some objective or evidential basis and not merely be unfounded rumour, gossip or supposition.

8.3 If a person has been interviewed under caution, arrested or processed through the criminal justice system (for example by use of PND or Street Bail) they MUST be recorded in the suspect or person page of the relevant core system.

8.4 In the case of a complaint being withdrawn or there is insufficient evidence all suspects **WILL** remain recorded and linked to the record with the relevant explanation being made in the notes.

All staff have a responsibility to ensure that the status of a person's suspected or actual involvement in a crime is updated throughout the investigation.

8.5 In the event of a crime record being filed as "No Crime", suspects will remain linked to the electronic crime report with a clear explanation in the notes as to the reason for "No Crime"

8.6 Suspects whose full names are not known will be entered into relevant operational systems in line with the Standard Operating Procedures for "unknown persons" relating to that system.

8.7 Where the only available information on a person is a notable description, then a record will be created with the description and every effort made to consolidate it into the correct person record as more information becomes available.

8.8 Where the suspect name is presumed to be a nickname or pseudonym (for example a name used on an internet social networking site) and the real name is not known, a unique person record should be created for the nickname or pseudonym (in accordance with the data quality rule in that system's Standard Operating procedure) in order to correctly categorise intelligence until a positive identification is made.

8.9 Suspects whose full names are not known will be entered into relevant operational systems in line with the Standard Operating Procedures for "unknown persons" relating to that system.

8.10 If, at any time in an investigation, details of the suspect are identified which identify that the person is already recorded on a force system (via a unique national identifier such as PNCID) , the suspect details will be updated with this information and/or merged with the existing golden person record.

Chapter Four

9. Review, Retention and Disposal

9.1 Records will be reviewed and either retained or disposed of in accordance with the force's current Review, Retention and Disposal (RRD) policy and Disposal Schedule.

9.1b The disposal policy will be adjusted to comply with the requirements of any official (national) inquiry into operational policing. Any alterations will be documented and signed off by a chief officer. All deviations from the RMS disposal policies (as detailed in this document) will be removed when the inquiry no longer requires this media be retained and on receipt of authorisation from a chief officer.

9.2 All records which are accurate, adequate, up to date and necessary for policing purposes, will be held for a minimum of seven years from the date of creation.

9.3 Records will be retained if one or more of the National Retention Assessment Criteria (NRAC), as detailed in the Authorised Professional Practice on Information Management are met.

9.4 Records will be retained, or disposed of in their entirety. Inaccurate entries within records must be corrected by way of additional clarification in order to maintain an audit trail.

9.5 Information is categorised into four groups, detailed in the appendices. Information will be retained for at least as long as the minimum stipulated by the Authorised Professional Practice on Information Management.

9.6 The force will aspire to compliance in the management, retention, review and disposal of information subject to the Authorised Professional Practice on Information Management.

- We will focus on ensuring that the quality of information entered onto our systems is accurate and timely.

- We will take a proportionate and risk tolerant view of the disposal of information, whilst acknowledging the legacy problems of existing systems

- We will take account of changing events such as the potential onset of national information systems and the implications of likely collaboration between two or more regional forces in our decision making

- Wherever reasonably possible we will ensure that any new systems are capable of being MOPI compliant in relation to the review and disposal of information

Part Three – Information & Toolkits

The information and toolkits section contains forms, letters, flowcharts, sample letters and application forms etc.

Appendix 1: Review Groups:

Review Group	Offence/Record Type	Action	Rationale
Group 1			
Certain Public Protection Matters	1. MAPPA managed offenders 2. Serious specified offences – CJA 2003 3. Potentially dangerous people	Retain until subject has reached 100 years of age. Review every 10 years to ensure adequacy and necessity.	This category poses the highest possible risk of harm to the public.
Group 2			
Other Sexual and Violent offences	Sexual offences listed in Schedule 3 Sexual Offences Act 2003 Violent offences specified in the Home Office Counting Rules/ National Crime Recording Standard	Review after an initial 10 year clear period. If subject is deemed to pose a high risk of harm retain and review after a further 10 year clear period.	National Retention Assessment Criteria – Appendix 4(i)
Group 3			
All Other Offences	Non-sexual, non-violent	Retain for initial 6 year clear period. Either review and risk assess every 5 years or carry out time-based disposal depending on force policy.	Lower risk of harm. Forces must balance the risk posed by this group with the burden of reviewing.

Group 4			
Undetected Crime	Serious specified offences. Other offences	Retain records for 50 years from the date the crime was reported to police. 6 years	CJA 2003 Limitation Act
CRB Disclosures	Information disclosed under Part 5 of the Police Act 1997	Retain for 10 years from date of request.	CRB Quality Assurance Framework
Intelligence Products	Target Profiles Association Diagrams	Review according to crime type as outlined in categories 1-3.	
Missing Persons	Resolved Unresolved	Retain for a minimum of 6 years. Dispose of if this period has been 'clear' and there are no further indicators of risk. Retain indefinitely.	Limitation Act 1980
Victim/Witness Details		Retain for a minimum of 6 years or length of sentence if this is longer. Decisions to dispose of must be made on a case-by-case basis. Retain if victim/witness is recorded as the offender/suspect for another offence.	Limitation Act 1980 CPIA 1996

A complete list of crimes and their associated review groups is available on the **Information Compliance Unit / Records Management Section** intranet site.

Appendix 2: Guidance on Managing databases

The following is brief guidance to ensure compliance with the Guidance on the Management of Police Information (MoPI) and the force Records Management Policy for databases and investigative products that are used to record and manipulate police information outside of the force's core systems.

This guidance is intended to complement the MoPI guidance, and the force's Records Management Policy which contains more detail on each of the areas.

Summary

Databases are allowed as long as they only contain information already held in a core system (if new information is added to the database this should be assessed for value and submitted to the appropriate area of a core database e.g. 839, crime report or task.

Each database must have a policy document stating the policing purpose for retaining this information in this format, security access arrangements and the planned review dates for the continued retention or disposal of this database. If in doubt contact the Records Management Section.

What is a database?

This guidance covers paper filing systems, databases on Excel or Access (sometimes even Word documents), Organisation Nominals within CONNECT and any policing information recorded outside of a core system. For the purposes of this document, all of the above will be termed "databases".

For the purposes of this guidance, such databases include commonly used applications such as Command and Control (to be replaced by Smart Contact), PentiP and Compact Missing Persons.

It is not intended to prevent the manipulation of existing data in order to conduct normal investigations, or create intelligence products, except where the database contains pieces of information which are relevant for a policing purpose and are not recorded within the core systems. If in doubt, contact the Records Management Section for advice.

Core Systems

The force's Core System remains the primary place to store policing information. These are the systems which directly feed the Police National Database (PND). Information stored outside of these systems is not available for disclosure and cannot be seen by other forces.

The Core System is CONNECT

Ownership

Any database that is created must be recorded by the Head of Information Compliance and have a senior named owner who is responsible for maintaining the database.

There should be a documented and published policy document making clear how the management of the database will comply with MoPI, Records Management Policy and any other legislation or guidance

Access

Access to records containing policing information, and especially those containing names, must be controlled to ensure that only staff with the appropriate access rights can access the database, and then only for a policing purpose. Advice on access levels and security can be found in the

Information Security policy, and guidance is available from the Information Security Officer.

Personal drives and shared public folders **must not** be used to store sensitive information.

Collection

Information must be collected and recorded only for a policing purpose as defined by MoPI.

- Protecting life and property
- Preserving order
- Preventing the commission of offences
- Bringing offenders to justice
- Any duty or responsibility of the police arising from common or statute law

Recording

Information should be recorded on the core system of CONNECT wherever possible. If information is missing from a core system, then a signpost must be added to it to inform internal and external users of the record that further information exists and how to access it. If there is an appropriate method of recording the information in question on a core system then it must be used. (e.g. investigations, arrests, PNCIDs and names all have proper fields or dedicated record types within CONNECT which must be properly used).

Care must be taken to ensure that the core systems are updated in a timely fashion with any relevant information.

Evaluation

Any information added to a database that is not already recorded within a core system must be evaluated in line with the requirements of the National Intelligence Model (NIM) and appropriately graded and submitted through the normal channels.

Information should be graded in accordance with MoPI as belonging to group 1, 2 or 3

Sharing

Information shared outside of the police service must be done in line with the Force's Information Sharing Policy. An Information Sharing Agreement should be created for third parties with whom information is regularly shared.

Any decision **not** to share information should also be recorded in line with the arrangements in the Information Sharing Policy, in order to identify the fact that sharing was requested, and the rationale for choosing not to share, in line with the guidance in the force Information Sharing Policy and MoPI guidance.

Review, Retention and Disposal

Policing Information should be regularly reviewed and, if not already done, transferred to a core system at the earliest opportunity.

Information should only be retained where there is a policing purpose to do so, and must be stored in a manner enabling it to be identified, located, searched on, and used operationally. If this cannot be done by means of transferring into a core system then a clear signpost must be placed on the master record (usually a CONNECT nominal).

Information should be disposed of when no longer held for a policing purpose. If the information on the database is a duplicate of information already held in a core system it may be disposed of. If any unique information has been added to the database the core system should be updated according to the guidance in this document.

The Records Management Section will review all information on core systems on behalf of the force. If information is stored outside of those systems the responsibility for MoPI review lies with the record holder.

MoPI Group 3 information should be disposed of after seven years, except where there is a continuing policing purpose to retain it for longer.

Other information must be regularly assessed using the National Retention Assessment Criteria (NRAC) form within the MoPI guidance (appendix 4(i)). A copy of the completed NRAC form should be retained, ideally with the record itself.

Policy Database Administration

For Policy Unit Use Only

Document information The table below lists the details relating to this document.

Item	Details	
Document Title	Records Management Policy	
Version	8.0	
Owner	Carol DUFF	
Author / Reviewer	Carol Duff Records Manager	
Date of last review	07/06/2018	
Date of next review	07/06/2021	
Risk Assessed	Completed:	Enter: Yes / No Yes
Equality Impact Assessment relevance test	Completed:	Enter: Yes / No Yes
Full Equality Impact Assessment	Completed:	Enter: Yes / No / Not relevant No
Compliant with Human Rights Act 1998	Enter: Yes / No Yes	

For Policy Authors Only

Revision information The table below details revision information relating to this document.

Topic Title	Date of last update
Minor amendments re CONNECT/Intel 5x3x2 system	07/06/2018