



Collection and Recording of Police Information Procedure

This procedure is part of North Yorkshire Police policy to which all Chief Constable personnel and the functions provided by the Deputy Mayor for Policing as part of the York & North Yorkshire Combined Authority are required to adhere.

Procedure Statement

Effective policing depends on efficient information management. The Authorised Professional Practice (APP) section on The Management of Police Information (MoPI) provides North Yorkshire Police (NYP) with guidance in relation to the collection and recording of information.

This is the overarching procedure produced to assist NYP in meeting MoPI requirements in relation to the collection and recording information. The procedure applies to all information identified for a policing purpose regardless of the format, system, or business area for which the information has been recorded.

In addition to the content of this procedure, individual business area process documents and guidance should be consulted for further detailed recording requirements. These must consider the requirements set out in this procedure.

Overarching Policies:

Records Management Policy
Information Security Policy
Data Protection Policy

Procedures:

Data Protection Subject Access Procedure
Freedom of Information Procedure
Management and Submission of Intelligence Information Procedure
Protective Marking Procedure
Safeguarding Children from Abuse Procedure
Domestic Abuse Procedure
Missing Person Policy
National Standards for Incident Recording Procedure
National Crime Recording Standards
Information Sharing Procedure
Information Audit Procedure

Review, Retention and Disposal of Information Procedure
Personal Data – Right to Rectification and Erasure Procedure
Data-Procedure

Other Documents:

APP Management of Police Information
APP Information Management Data Protection
Niche Records Management System – User Guides
Information Management Site

Process

The accurate and timely collection and subsequent recording of police information is vital to effective policing. When information is collected it is essential that it is processed accurately and in line with legal and statutory requirements.

Police Information

Police information is information processed for a policing purpose. A policing purpose may include one, or a combination of the following (refer to APP Intelligence management).

- 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

If there is no policing purpose, then the information cannot be held as police information.

To assist in the lawful management of police information the requirements of the Human Rights Act (HRA) 1998 and Data Protection Act (DPA) 2018 need to be met. It should also be noted that any subject of information can have access to it at their request and that information is accessible to other key partners and the public through Information Sharing Agreements and legislation such as the Freedom of Information Act (FOI) 2000.

Collection of Police Information

Police information is collected through a number of ways, defined in APP MoPI as:

- **Routine** – where information is collected as part of routine policing activity
- **Tasked** – the prioritised collection of information, for example problems and subjects (suspect or victim) identified in the intelligence requirement. Refer to APP Intelligence management
- **Volunteered** – information that is received which may not fall into routine or tasked information, it is usually collected from other agencies, partners, and the general public

Recording Police Information

The creation of a record (in the appropriate format) enables information to become a corporate resource. Failure to record information accurately will impact on effective management of risks posed to the public and police; cause the misdirection of resources and non-compliance to national standards.

Information from key business areas (for example, crime, intelligence, domestic abuse, child abuse and custody) is uploaded onto the police national database (PND). Information is also extracted and uploaded to share with other agencies such as Disclosure and Barring Service (DBS) through the Police Local Exchange (PLX).

In line with APP MoPI, information (where recording systems allow) should be categorised in terms of people, objects, locations, and events (POLE). In relation to police information person records do present the highest risk and personal information must be processed in line with legal requirements.

The person responsible for the recording or the submitting of information for subsequent recording of the information (depending on business process) must have regard to the recording principles as set out in the APP MoPI:

- police information must be created for a policing purpose
- comply with data quality principles and Data Protection principles particularly in respect of processing personal data
- identify who completed the record, when and for what purpose (audit trail)
- checks should be made in other business areas to see whether the information is already held to help avoid unnecessary duplication
- if information is already held on an individual, then the existing record should be updated
- if it is identified that the information is connected to other information then it must be appropriately linked
- police information must be recorded as soon as practicable in accordance with the standards relating to the business area in which the information is held
- consideration should be given to the application of the appropriate Government Security Classification (GSC)
- where appropriate, the source of information should be recorded to ensure accuracy and to assist in requesting further information

Person Records

Person details should be as complete as possible and efforts made to establish a person's identity, emphasis is made on making a person's record unique so that all information about a person can be linked to one record.

It is accepted that in some cases it is not always possible or relevant to obtain full details and consideration must be given to the application of Article 5 (1) (c) of the General Data Protection Regulation (GDPR) and the third Data Protection Principle under Part 3 Law Enforcement Processing of the Data Protection Act 2018; that personal data must be adequate, relevant, and not excessive in relation to the purpose for which it is processed.

Creation and update of a person record

Before creating a new person record a review must take place to ensure the person record does not already exist.

When considering whether the information should be linked to an existing record or a new unique record created, the following minimum matching criteria should be applied:

- Forename, and
- Surname, and
- DOB and
- One other distinguishing piece of information for example address, telephone, email address or another identifiable piece of information e.g. PNCID, Driving Licence number etc.

This reduces duplication and supports the ability to link all information to one single record. This criteria is known as the minimum data set or 3+1.

Once it is established that a new record needs to be created the process for creating a new record should be followed. The greater the detail obtained about a person, the greater the likelihood the record will be unique.

When creating a person record, APP MoPI advises that it should contain, as a minimum one of the following:

- Forename
- Family name
- Partial name
- Nickname
- Alias

This minimum requirement is more likely to apply to intelligence or suspect information.

Other desirable basic fields to add to a record as outlined in APP are:

- Sex
- Ethnic origin
- Height

How a person or a vehicle / object are linked to information must reflect the actual involvement accurately. The sharing of information nationally and with other agencies relies on the accuracy of the relation type. Further guidance will be provided for STORM and Niche recording.

The table below provides clarity on how records should be recorded for Officers/Staff on Niche:

Circumstances	Niche Staff Record	Niche Personal Record
Officer/Staff Victim ON Duty		X
Officer/Staff Victim OFF Duty		X
Officer/Staff Witness ON Duty	X	
Officer/Staff Witness OFF Duty		X
Officer/Staff Suspect ON Duty		X
Officer/Staff Suspect OFF Duty		X
Officer/Staff submits Intel ON Duty	X	
Officer/Staff submits Intel OFF Duty		X
Officer/Staff Reporting Person ON Duty	X	
Officer/Staff Reporting Person OFF Duty		X

ACL (Access Control Level) Records

There is sometimes a need to restrict access to Niche Occurrences in certain circumstances. ACLs are used for the protection and management of restricted data within NYP. The purpose of this restriction is to protect vulnerable individuals, communities or other parties should information relating to this incident become known within the organisation. This not only protects those listed above but also provides NYP an additional enhanced level of protection

Criteria for restricting Crime and General Occurrences

Occurrences should only be restricted where absolutely necessary and for an agreed legitimate policing purpose. As a general rule occurrences falling within the below criteria should be restricted:

- Occurrences involving NYP serving officers, current NYP staff or where appropriate their immediate family members where the unrestricted access to the occurrence would cause safeguarding, integrity, or crime prevention issues for those involved or NYP.
- Occurrences involving a high-profile public figure or a high profile operation where unrestricted access could compromise NYP's integrity

- Kidnap occurrences
- Extortion/Blackmail Occurrences
- Honour Based Incidents
- Occurrences related to Witness Protection
- Occurrences related to Covert Operations and Security Operations
- Occurrences involving NYP serving officers, current NYP staff or where appropriate their family members where the unrestricted access could cause embarrassment through other people in NYP seeing private information about a colleague.

Where this is identified, an ACL can be applied. Niche Systems Admin will send the details to the Head of Professional Standards Department within 72 hours to determine if an ACL remains appropriate. The Head of PSD will decide if this is to remain in place and for how long. Commonly, this is to ensure that the person's own colleagues do not read information which would not otherwise be available in the workplace. However, this will be balanced with any ongoing safeguarding needs and the assessment as to at which point this must become visible for any circumstances where the same individual comes to police attention again, so the attending officer / staff can understand the background, and in the case of local policing teams, them being aware of where vulnerabilities are. Keeping a log restricted to avoid embarrassment must not be counter-productive to safeguarding.

Occurrences should remain restricted only while the criteria listed above still apply (Intelligence occurrences will have separate ACLs applied as appropriate to meet sensitive operational needs). Access to ACL'd occurrences will be granted when appropriate. To request access to restricted records where appropriate during working hours please email Niche System Admin. For out of hours requests please contact the Force Incident Manager.

Data contained within restricted occurrences is not restricted on PND and can be viewed by all users. The following types of occurrences have been identified as requiring additional level of restriction for PND and a DARC 5 marker is placed on the following occurrence types:

- Kidnap occurrences
- Extortion / Blackmail occurrences
- Honour Based incidents
- Occurrences relating to Witness Protection
- Occurrences relating to Covert Operations or Security operations
- Occurrences that relate to high profile public figures or high-profile operations

Quality Assurance

Regular monitoring should be undertaken by supervisors to ensure that staff members responsible for the collection and recording of information follow the standards set out in this procedure and other related guidance documents.

Data Quality reports (prioritised by risk) are produced, and actions carried out in order to improve the overall accuracy of the recorded police information (see Data Procedure)

Responsibilities

Operational officers/police staff / users with write access to police recording systems

Awareness of the need to collect and record police information in accordance with legislation and guidance including DPA and the Information Management section of APP. Provide accurate and comprehensive updates in the appropriate format. Ensure inaccurate or out of date information is amended. Where possible ensure person records are unique. Ensure links and involvements are recorded and reflect the circumstances accurately. Respond to reasonable requests for clarity or further information in relation to the recording of police information.

First Line Supervision

Ensure staff receive appropriate training to fulfil their role effectively and that they are fully aware of the need to record information accurately and the impacts of not doing so. Regularly monitor work completed by staff in relation to the collection, submission and recording of information, to ensure compliance with data quality and recording principles. Provide appropriate feedback and take appropriate action for non-adherence where necessary.

Heads of Department / Commanders

Promote effective Information Management ensuring teams comply with the standards for the collection and recording of police information. Ensure that data quality is treated as a priority. Manage the performance of staff in aspects of non-adherence.

Users with Read Access

Where appropriate, provide updates to information using the appropriate method if it is identified that information is out of date or inaccurate.

Collection and submission of relevant and accurate information through the appropriate process to support effective recording of Police Information.

System Administrators

Provide the relevant points of contact across the organisation with information in relation to system changes that may affect the collection and recording of police information. Review requests to merge, amend, delete information, and provide assistance and reports where necessary.

Training Services

Ensure that staff are provided with relevant level of training to perform their role in a timely manner and that lesson plans are up to date.

Information Management

Provide support in relation to the Code of Practice for the Management of Police Information for the collection and recording of police information. Provide advice as part of the change management process ensuring that effective police information management is maintained, and impacts highlighted where necessary. Provide activity analysis data, providing solutions to assist in performance improvements.

Chief Officer Team

Promote effective Police Information Management by having overall responsibility for ensuring staff adhere to best practice in relation to the Collection and Recording of Police Information and ensure that data quality is treated as a priority.

Definition of Special Terms

APP	Authorised Professional Practice
DPA	Data Protection Act 2018
FOI	Freedom of Information
GDPR	General Data Protection Regulation
NSIR	National Standard for Incident Recording
NCRS	National Crime Recording Standards
MoPI	Management of Police Information
HRA	Human Rights Act
GSC	Government Security Classification
DoB	Date of Birth
PNC	Police National Computer
PLX	Police Local Exchange
POLE	Person, Object, Location Event
PND	Police National Database
DQ	Data Quality