



Review, Retention and Disposal of Information Procedure

This procedure is part of North Yorkshire Police policy to which all Chief Constable personnel and the functions provided by the Police, Fire and Crime Commissioner are required to adhere.

Procedure Statement

The inquiry by Sir Michael Bichard, following the murder of Holly Wells and Jessica Chapman in August 2002 by Ian Huntley, led to the Home Secretary issuing a statutory Code of Practice on the Management of Police Information (MoPI) with which all forces are required to comply. This includes the requirement to review information held so that informed and risk-based decisions can be made whether to retain or dispose of information.

The UK GDPR and the Data Protection Act 2018 require that personal data held is managed in line with Data Protection Principles. Of particular relevance to RRD is that personal data must be accurate, relevant to our lawful purposes, limited to what is necessary, and must not be kept for longer than we need it.

The Information Management section of the College of Policing (CoP) Authorised Professional Practice (APP) provides a detailed framework for managing crime and offence-related records, and directs forces to the relevant national guidance in relation to the management of other policing and corporate information.

This procedure aims to provide guidance on the review, retention and disposal of information to assist the organisation in meeting national and legislative requirements including the Human Rights Act 1998 (HRA), Criminal Procedure and Investigations Act 1996, The Freedom Of Information Act 2000 and Data Protection Act 2018 (DPA).

While this procedure is extensive, there may be exceptions or omissions in relation to the information obtained, held and processed by NYP. In such cases, it is the responsibility of individual officers and staff to highlight the need for amendment to the procedure and inform the Procedure Author.

Overarching Policies:

Records Management Policy
Data Protection Policy
Information Security Policy

Other Procedures:

Collection and Recording of Police Information
Personal Data – the right to rectification and the right to erasure
Deletion of Records from National Systems Procedure
Property & Exhibits Procedure (Appendix D)
Property (Lost & Found) Procedure

Other Documents:

College of Policing MoPI APP - Retention, review and disposal
NYP Retention Schedule
Operational Paper File Management Guidance
RRD summary – outline of why and how we retain information
Quick Reference Guide to Reviewing the Retention of Digital and Physical Evidence
Information Asset Management
ICO guide to deleting personal data 2014 (ico.org.uk)

Process

Our responsibilities under the Data Protection Act/UK GDPR and MoPI apply during the whole lifecycle of a record or piece of information, from when we first receive or collect it through to its disposal.

Review, Retention and Disposal (RRD) requirements should be considered at the point of development of new systems and working practices. In many cases this will be addressed as part of a Data Protection Impact Assessment (DPIA) or Data Processing Contract (DPC), but RRD must also be considered for minor changes in the way information is handled, such as setting up a new team site or changing a storage location. Where RRD is not being managed centrally, Business Area teams should be aware of RRD requirements for the records they manage, and put appropriate administrative processes in place to manage these.

Staff and officers recording information on NYP systems must be doing so only for policing or other lawful purposes, and must be aware of and comply with team processes in place to support the effective management of that information.

To support effective RRD, recording practices must be in line with the Collection and Recording of Police Information Procedure, and team processes in relation to accuracy of information and data quality should be documented so that staff and officers are clear on the requirements of their role.

RRD Process by information type**Crime/Offence-related information**

For the RRD of crime/offence related information we differentiate between 'Records' and 'Digital and Physical Evidence', as different retention rules and guidance apply:

Crime/offence-related records are retained in order to support the management of risk and comply with relevant legislation. Information that allows us to identify persons, objects, locations and events, and which contributes to understanding the nature of a crime or offending behaviour and the risk posed, is retained under MoPI.

College of Policing Authorised Professional Practice on the Management of Police Information (MoPI APP) – Review, Retention and Disposal (RRD) section applies.

Digital and Physical Evidence (DPE) is any physical property or digital data/media downloaded or recovered which could potentially form part of the evidence of a criminal offence and which may become a court exhibit in any judicial proceedings, or CPIA-relevant unused material. The purpose of retention here is to support and safeguard the criminal justice process.

Criminal Procedure and Investigations Act 1996 (CPIA) & NPCC National Digital and Physical Evidence Guidance apply.

Where material is both a record and an exhibit/evidence (eg witness statements), MoPI retention will apply. MoPI retention periods always exceed CPIA requirements.

Crime/offence-related records

These are records which relate to criminal or offending behaviour, including alleged or suspected criminal or offending behaviour, for example crime and investigation records, custody records and intelligence reports.

The review and appropriate retention/disposal of crime and offence-related police information is central to risk-based decision making, public protection and legal compliance.

Records must be regularly reviewed to ensure that they remain necessary for a policing purpose, are accurate, adequate and up to date, and are kept for no longer than is necessary.

MoPI groups 1-3 are applied to these records, dependant on the nature of the crime or offending behaviour, and retention decisions are risk and person-based.

In North Yorkshire Police these records are stored and managed within Niche where possible.

INITIAL AND TRIGGERED REVIEWS

At the point information is input into an NYP system, it should be risk assessed, taking into account other available information, and then evaluated to determine its provenance, accuracy, relevance to a policing purpose and the action necessary. This should be undertaken by the person or team inputting the information.

When further information is recorded relating to an individual, the business area recording the information should take reasonable steps to ensure the record is as accurate and up to date as possible, and address any data quality issues identified.

Unless confirmed as inaccurate, existing information should not be deleted from the system, as this information may be relevant in the future.

Information confirmed as inaccurate should be promptly updated/corrected/supplemented as appropriate whilst ensuring that an audit trail of the record history, and any inaccuracies that may have been viewed/used/shared while present on the system, remains on the record. *See also 'Inaccurate Information' section below.* Deletion of Niche records (other than by the record creator within the configured 'grace period') are handled by Niche

Systems Admin, who will seek specialist advice from line management and/or Records Compliance where necessary.

Any requests from data subjects for the Rectification or Erasure of records under the Data Protection Act 2018 must be referred to Records Compliance.

SCHEDULED REVIEW

Scheduled RRD assessments and related activity are carried out by the Niche RRD team in accordance with College of Policing MoPI APP RRD section, and Niche RRD team guidance.

The retention assessments carried out by the Niche RRD team will include checking that:

- there is a continuing policing or other lawful purpose for holding the record;
- the record is adequate, up to date and not excessive;
- the processing of personal data complies with the principles of the Data Protection Act 2018;
- the correct MoPI group/grade has been applied to the record, based on the information available

This is a specialist assessment and decision-making process, which may require consideration of all NYP and nationally held records relating the person, and should not be completed by other teams without consultation with Niche RRD/Records Compliance.

Teams storing MoPI group 1-3 records outside of Niche, but which relate to a Niche occurrence should either reference their record on the Niche occurrence (so that the RRD Team are aware of this) or liaise with the Niche RRD team as necessary to ensure their records are retained and disposed in line with the Niche record.

Teams storing MoPI group 1-3 records separately with no corresponding Niche occurrence must ensure that their record retention is aligned as appropriate with any records on Niche which relate to the same nominal(s), and that the full picture of any risk posed is accessible to colleagues in other teams as and when necessary. In addition to supporting operational risk management, this is necessary to inform accurate MoPI reviews, and for Data Protection Act compliance.

Exceptions to the above should be risk assessed, approved by Information Management, and documented on the Force retention schedule by Records Compliance.

Crime/offence-related Digital & Physical Evidence

Digital and physical evidence should be reviewed for retention and disposal by the OIC in line with their CPIA responsibilities, and with consideration of the NPCC National DPE Guidance. Operational management/supervision must ensure that appropriate and CPIA-compliant arrangements are in place for material to be reviewed where the original OIC is unable to do this or no longer in post.

Digital and Physical Evidence held in the property stores should be managed in line with the Force Property and Exhibits Procedure. Guidelines to assist officers in meeting the CPIA and DPE requirements are provided in Appendix D.

Digital and Physical evidence held elsewhere within force may have additional business-specific retention requirements and guidance, but processes should be compliant with the National DPE

Guidance and/or aligned with the Property and Exhibits process where possible. Business area/team guidance and processes should be developed in consultation with all relevant stakeholders and Records Compliance/Information Assurance Board as appropriate; approved by Exhibits and Property Board; and documented in the Force Retention Schedule.

Some ancillary records may be treated as evidential material rather than records requiring MoPI retention, providing they do not contribute to the long term management of the risk posed by the individual, for example records of workflows/processes used to generate digital evidence.

Information gleaned from evidential material that contributes to the long term management of the risk posed by the individual should be present on Niche (or other operational record system as appropriate) for MoPI group retention. This could be in the form of an MG11, OEL notes, warning marker/flag etc. The provenance of such information should be recorded, even where we are not retaining the original exhibit.

Other Policing Purpose information

These are records processed for a policing purpose, but which do not relate to crime or offending behaviour. They include Missing persons, RTCs (where no offending is present or suspected), general occurrences, licensing records, and any other information processed for a policing purpose which does not fall under MoPI groups 1-3. The Review, Retention and Disposal of Other Policing Purpose records should be managed in line with the Force Retention Schedule

In NYP, 'other policing purpose' records on Niche will be reviewed centrally by the Niche RRD team. Exceptions should be by agreement between Information Management and business areas, depending on business-specific requirements.

Related records held by teams locally should be retained/disposed in line with the Niche record.

Where there is no Niche record, review and retention must be managed by the business area/team on behalf of their Information Asset Owner/SIRO. See the 'Developing Business Area processes' section below.

Property relating to 'Other policing purposes' is managed in line with the Force Property and Exhibits Procedure/Lost and Found Property Procedure.

Corporate Records

The Review, Retention and Disposal of Corporate records must be carried out by the Business area responsible for the records. The NYP Retention Schedule provides minimum retention periods and guidance notes, and teams should have local processes in place to manage the Review Retention and Disposal of their records in line. See the 'Developing Business Area processes' section below.

Material required for Inquiries

Records which may be relevant to an ongoing National Inquiry must be retained until the Inquiry instructs the force they no longer need to retain these (Inquiries Act 2005). Retention may also be extended for the purposes of local inquiries or investigations. If the information would otherwise be disposed, the purpose of retention must be documented at review, and further review scheduled to ensure that any personal data is not retained for longer than necessary.

Duplicate and Working Copies

There are no separate retention requirements detailed in CPIA/MoPI/DPA or related Information Management guidance for duplicate/working copies. These must be managed locally by Business Areas to meet their policing or corporate needs, taking into account any relevant national guidance and best practice specific to their business area, and any reference therein to the handling or retention of duplicate/working copies.

Teams which create, store or share copies of records or evidence must have systems in place to ensure that when the master copy is due for disposal any remaining copies can be located and disposed at the same time.

Paper records

Please refer to the Operational Paper File Procedure in relation to information retained for a policing purpose. For Corporate information, where it is necessary to retain paper records, these should be reviewed and disposed in line with the retention schedule as per electronic records.

Records held in National Systems

Records held in National Systems may be subject to different RRD rules and processes. Eg. PNC; ViSOR; PENTIP; HOLMES; NFLMS.

Management of these records by NYP will depend on whether we are the Data Controller for that information, what additional legislation applies, whether there are National or Regional agreements in place, and any relevant Data Processing Contracts/Information Sharing Agreements.

Please seek advice from line management or the Data Protection Officer/ Compliance Team if you are unsure of your team's responsibilities in relation to the management of data on National or Regional systems.

Other retention purposes

The Data Protection Act allows for extended retention of personal data for public interest archiving, scientific or historical research, or statistical purposes, subject to appropriate safeguards to protect the data subject. Any retention of personal data for these purposes on NYP systems beyond the MoPI or Retention Schedule periods must be documented and agreed with the Compliance Team, to ensure appropriate checks and measures are in place.

Inaccurate information (all record types)

Inaccurate information should be promptly updated/corrected/supplemented as appropriate whilst ensuring that an audit trail of the record history and any inaccuracies that may have been viewed/used/shared while present on the system, remains on the record. Consideration must be given to how inaccurate information may have been used or shared. Advice must be sought from Operational line management, Records Compliance or Information Security as appropriate. Information Security incidents resulting from inaccurate data (eg correspondence sent to the wrong address) must be reported in line with the Security Incident Reporting Procedure.

Developing Business Area RRD processes

Where RRD is not managed centrally, business areas should develop and maintain processes to manage the RRD of their records as per the requirements detailed above for different information types.

If records are crime/offence-related, or relate to Niche records, teams must liaise with Records Compliance and Niche RRD to align or integrate processes as necessary for MoPI compliance.

If records are held for a DPA Law Enforcement purpose outside of Niche, teams should consult with Records Compliance, as these may carry additional logging requirements under the Data Protection Act.

For all other records (ie 'Other Policing Purpose' outside of Niche, and 'Corporate'):

- Team guidance, and any detailed local schedules as required, should be developed in line with the Force Retention Schedule, or in consultation/agreement with Records Compliance.
- Teams should have documented review periods and retention criteria/considerations for each type of record.
- Review and disposal activity in relation to records containing personal data should be logged for audit and monitoring purposes:
- Where a record is reviewed and retained, the rationale for retention should be recorded and a new review date set as appropriate.
- Where a record is disposed the review and outcome should be logged for audit and monitoring purposes, but no personal data should remain on the record or the log

Please consult with Records Compliance if advice is needed to develop and document processes.

Disposal of information

Personal data and operationally sensitive information must be managed and disposed in line with our Information Security Policy at all times.

Business areas storing and managing their own records should have disposal processes documented within their RRD process.

Once we no longer have a policing or other lawful purpose for retaining personal data it should be permanently deleted/destroyed.

Paper records containing personal data or operationally sensitive information must be disposed via our contracted confidential waste disposal: Confidential waste bins are located and clearly marked within NYP buildings.

Personal data or operationally sensitive information held in digital/electronic systems, devices or media should, where possible, be irretrievably deleted, ie deleted/securely overwritten/sanitised as necessary to ensure that it cannot be recovered. Advice must be sought from ICT and Compliance Team as necessary to implement this. Where it is not technically possible to fully delete, the data must be put 'beyond use': advice must be sought as necessary from the Compliance Team/Information Security and ICT, and arrangements must be documented on the relevant DPIA/DPC/SIRO Assurance statement.

Disposal of Niche records

Deletion/disposal of Niche records is managed by the Niche Team (Niche Systems Admin & RRD). Work is ongoing with Minerva and Niche Technologies to develop automated processes for the review and deletion of Niche records where appropriate. In the meantime records identified for disposal will be considered and managed on a case by case basis by the Niche RRD Team.

Disposal of Property and Digital/Physical Evidence

Property and evidence retained in central stores will be disposed by Exhibits Management in line with the Property and Exhibits Procedure and related guidance. Business areas storing physical or digital evidence locally should have disposal processes documented within their team processes or guidance.

Risk/mitigation

Areas of non-compliance with the above procedure should be reported to the Compliance Team, to be considered for recording on the risk register.

Responsibilities

Niche RRD Team

- Undertake reviews of Niche records in line with APP MoPI. Accurate recording of such activity to meet audit and legislative requirements.
- Review and respond to Data Protection Act Requests for Erasure of Niche and related operational records, in line with Personal Data – the right to rectification and the right to erasure

Records Compliance Team

- Maintain and update the NYP Retention Schedule
- Provide advice in relation to RRD requirements and the development of RRD processes
- Receive, review and respond to Data Protection Act Requests for Erasure of records held by NYP, in line with Personal Data – the right to rectification and the right to erasure
- Record areas of risk in relation to the RRD of information

Operational Officers/Police Staff

- Maintain awareness of Data Protection Act 2018 responsibilities in relation to the personal data that you process and complete any relevant mandatory training.
- Maintain awareness of this procedure and comply with your business area/team processes for the RRD of the records you deal with.
- When adding information to crime or offence-related records, apply *initial* review considerations as detailed in this procedure.
- Liaise with Niche RRD as necessary and as requested, to support the centralised MoPI RRD process, and carry out deletion activity on request of the RRD team when locally-held records are identified for disposal.
- Undertake review and disposal activities in relation to records managed by your business area/team in line with this procedure, agreed business area/team processes and the NYP retention schedule.

- Inform Records Compliance as soon as possible if you receive requests for rectification or erasure of records, either written or verbal: Personal Data – the right to rectification and the right to erasure

First Line Supervision

- Ensure that team members are aware of and supported to comply with the requirements of this procedure and the Data Protection Act.
- Ensure that appropriate team processes are in place for the RRD of information held by local business areas/teams, in line with this procedure.

Information Asset Owners

- Ensure that appropriate Review, Retention and Disposal arrangements are in place for the information assets you own
- Advise the Compliance Team of any changes in asset retention/processes so that the Information Asset Register can be updated

Commanders/Heads of Department

- Ensure that team members are aware of and supported to comply with the requirements of this procedure and the Data Protection Act.
- Ensure that appropriate team processes are in place for the RRD of information held by local business areas/teams, in line with this procedure
- Ensure your team's Data Protection documents are updated as requested by the Compliance Team (*Information Asset Register entries; SIRO Assurance Statements; and Data Protection Impact Assessments/Data Processing Contracts*), to support compliant RRD processes, and related risk management.

Chief Officer Team (COT)

- Overall responsibility including the roles of Chief Information Officer and the Senior Information Risk Owner
- Promote and support efficient RRD processes

Definition of Special Terms

APP - Authorised Professional Practice

COT - Chief Officer Team

CoP - College of Policing

CPIA - Criminal Procedure and Investigations Act (1996)

DPA - Data Protection Act (2018)

EPB - Exhibits and Property Board

HOLMES – Major Crime national database (Home Office)

IAB - Information Assurance Board

Minerva – Collaboration programme between all Niche forces

MoPI - Management of Police Information

NFLMS – National Firearms Licensing Management System database

PentiP - Penalty Notice Processing

PNC - Police National Computer

RRD - Review Retention and Disposal

ViSOR - Violent and Sexual Offender Register

Data Protection Act lawful purposes *(for processing personal data):*

- (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.*
- (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.*
- (c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).*
- (d) Vital interests: the processing is necessary to protect someone's life.*
- (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.*
- (f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)*

DPA Law Enforcement Purpose: *The prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'*

MoPI Policing Purposes *(for retention of policing information - College of Policing MoPI APP) :*

- a) Protecting life and property;*
- b) Preserving order;*
- c) Preventing the commission of offences;*
- d) Bring offenders to justice;*
- e) Any duty or responsibility of the police arising from common or statute law.*