Review, retention and disposal

This page is from APP, the official source of professional practice for policing.

First published 23 October 2013 Updated 16 August 2023
Written by College of Policing
49 mins read

Purpose and scope

This authorised professional practice (APP) provides guidance to forces on meeting the requirements of the **Police information and records management Code of Practice** in relation to the review, retention and disposal of policing information and records. This APP is supplemented by the Manual of Guidance (currently under development), which provides a further level of operational data.

The retention, review and disposal regime relates to policing information held on individuals (nominals) who have come to the notice of police as offenders, suspected offenders or whose details have been recorded for another policing purpose (definition below).

When referring to ‘nominals’, it is important to consider the special issues that can arise when a record includes details of a child under 10. A child under 10 cannot be found guilty of an offence but may still be a risk to the public or themselves, or the retention of their record may otherwise serve one or more policing purpose. Subject to having an underlying policing purpose, it could be necessary and proportionate to retain a child’s record, whether as a victim, witness, informant or suspect. In reaching that decision, decision-makers will need to consider the full circumstances and bear in mind the requirements of section 11 of the Children Act 2004 regarding the duty to have due regard to the child’s safeguarding needs. Further specific guidance is set out below.

Throughout this guidance there is reference to nominals, suspects, offenders and suspected offenders. Children under 10 who are suspected of behaviour that, if committed by a person over 10, would be criminal conduct are included in those terms.

There is a subset of policing information and records that relates to evidential material. This refers to any physical property, digital data or media that is downloaded or recovered, could form part of

the evidence of a criminal offence and may become a court exhibit in any judicial proceedings. This could include downloads from mobile phones, body-worn video footage and CCTV. This definition applies to both digital and physical evidence.

Any unused evidential material should be examined as part of a robust post-case review and consideration should be given to the need for retention or disposal under the Criminal Procedure and Investigations Act (CPIA) 1996. Other evidential material should be retained in line with this APP. However, forces should work towards systems and processes that will allow the efficient deletion of evidential material within the CPIA 1996 timescales, in line with the **National Police Chiefs' Council (NPCC) advice**. Note: the link is accessed via log in to the Knowledge Hub.

Metadata relating to digital material should be retained under MoPI as part of the record.

It should also be noted that the retention periods for biometric data are governed by the **Protection of Freedoms Act 2012** and sit outside this APP. The NPCC has published **guidance on the retention, storage and destruction of materials and records related to forensic examination**. (This guidance is hosted on the **Forensic Capability Network library**.)

The review, retention and deletion process as described in this APP and in the Police information and records management Code of Practice does not apply to the deletion of information and records held on the Police National Computer (PNC).

There are two types of information held by the police service.

- Policing information is information held for a policing purpose. The Police information and records management Code of Practice definition of 'policing purpose' is:
  - 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
- Corporate information includes other organisational information, such as human resources (HR) or finance records, minutes of meetings, policies and procedures.

For review, retention and disposal procedures, policing information is further separated into what can be described as offending behaviour (‘crime or offence-related’) and ‘other’. This is further described below.

Policing information

Crime or offence-related

Crime or offence-related information relates to criminal or offending behaviour, including alleged or suspected criminal or offending behaviour. This can include information in records such as crime records, records of investigations, custody records and intelligence reports.

The purposes of review, retention and disposal procedures for crime or offence-related police information is to:

- protect the public and help manage the risks posed by known offenders and other potentially dangerous individuals
- ensure compliance with the relevant legislation

The review of crime or 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.

All decisions related to the review, retention and disposal of crime or offence-related police information should be made in line with this section of APP.

Other police purpose

Other police purpose information is obtained or recorded for a police purpose that is not related to crime or offending behaviour, such as missing people, lost and found property, licensing records, event notifications and road traffic collisions (where there is no indication or suspicion of offending behaviour).

Guidance on the retention of these records can be found in the **NPCC National Retention Schedule (NRS)**.

Corporate information

This is information contained within records that do not have a policing purpose. It should be noted that records and information that relate to crime investigations, such as Gold Group meetings, should be retained in line with the appropriate MoPI crime category as described in this APP. Where crime or offence-related information is contained within corporate records, the relevant extracts should be copied or removed and included within the crime case papers.

Corporate and organisational records held by police forces should be retained for as long as they serve an organisational purpose or in compliance with rules, regulations or legislation. Wider public interest issues may necessitate extended periods of retention. Guidance on the retention of these records can be found in the NPCC NRS.

Where records are required to be retained under specific legislation (for example, the **Inquiries Act 2005**), they should be flagged as such. When these records are no longer required for a policing purpose, they should only be accessed for purposes related to the Inquiries Act 2005 or in response to freedom of information (FOI) requests. Arrangements should be put in place to manage such archived records, to ensure that they are held securely and disposed of when no longer required for the purpose for which they were retained.

Forces should record their approach to review, retention and disposal of all police records, including approaches to risk and risk mitigation. The force's senior information risk owner (SIRO) should understand the extent of each risk, and information asset owners (IAOs) within the force should be identified.

Retention

Retaining information relating to offending behaviour helps forces to prevent and detect crime and to protect the public. However, retaining every piece of information collected is impractical and unlawful. Consideration must be given to the types of information that need to be retained, the length of that retention and the practical implications of storing these records in their various formats. All reviews that result in a decision to extend the minimum retention of records must be recorded on a **national retention assessment criteria (NRAC) template**.

The processing of information and records management in the service is subject to a number of statutory obligations and standards. This APP should be considered in conjunction with all relevant legislative and regulatory requirements, including – but not limited to – the following.

- Police information and records management Code of Practice.
- Data Protection Act (DPA) 2018.
- Human Rights Act 1998.
- CPIA 1996.
- Protection of Freedoms Act 2012.
- Regulation of Investigatory Powers Act 2000.
- Freedom of Information Act (FOIA) 2000.
- Children Act 2004.
- Equality Act 2010 (including the public sector equality duty under section 149).
- Other codes, such as the Code of Practice on the Management of Records issued under s46 of the FOIA 2000 and the Surveillance Camera Code of Practice 2013.

When carrying out a review, and deciding whether to retain information, the decision-maker must consider, as a whole, the circumstances of the recorded event(s) and the characteristics of the nominal. For example, it is recognised that, even when taking into consideration the section 11 Children Act 2004 requirement to consider the need to safeguard and promote the welfare of children, it may be necessary to retain a crime record relating to a child under 10. This is for the purpose of their safeguarding and to manage any risk of harm to the public or victims/witnesses. The reason for the decision in these circumstances should be recorded.

The decision to retain is iterative and the same considerations apply for each review.

Some key points to consider when managing the review, retention and disposal of police information are:

- adherence to the principles in the Police information and records management Code of Practice
- the policing purpose that justifies retention
- the use of the NRAC when reviewing records
- other risks or time factors not included within the NRAC assessment, such as crime types of concern to a force
- the appropriate method for storing, accessing and retrieving records, taking into account the Government Security Classification (GSC)
- information retained must be easily searchable and retrievable by staff who are appropriately vetted and have a legitimate purpose

- information should be retained in accordance with National Police Information Risk Management Team (NPIRMT) Community Security Policy
- forces can use archives with limited access to store records, but this is not to be used for information that must be disposed of
- CPIA 1996 requirements:
  - the retention periods imposed by the CPIA are a minimum requirement and, in most cases, the retention requirements outlined in this **APP** will far exceed those imposed by the CPIA
  - information and records that fall within the remit of this APP should still be retained for as long as it is necessary and proportionate to do so, irrespective of the CPIA requirements for it
- forces should ensure that they understand the specific requirements of the Inquiries Act 2005 for any ongoing public inquiry, considering both relevancy and proportionality in any decision making
- section 11 of the Children Act 2004 requires that the chief officer of police for the police area makes arrangements for ensuring their functions are discharged having regard to the need to safeguard and promote the welfare of children (this responsibility, although expressed as applying to chief officers, also applies to officers and staff carrying out functions on behalf of the force, including the review, retention and disposal function in forces on behalf of the chief officer)
- the public sector equality duty in section 149 of the Equality Act 2010 requires that a public authority must, in the exercise of its functions, have due regard to the need to:
  - (a) eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under the Equality Act 2010
  - (b) advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it
  - (c) foster good relations between persons who share a relevant protected characteristic and persons who do not share it

Review

Reviewing information held by forces to determine its adequacy, relevance and continuing necessity for a policing purpose is a reliable means of meeting the requirements of DPA 2018. Review procedures should be:

- practical and proportionate
- risk-focused

- able to identify valuable information
- as straightforward as is operationally possible.

This APP details standard procedures in place for reviewing records and making accountable decisions on the retention or disposal of information.

All person records held by the police service should be subject to:

- a standard process for reviewing
- a data quality assessment

For audit and supervision purposes, a record must be kept of every review undertaken, irrespective of whether it results in any alterations or disposal.

Any record that is deemed to include inaccurate information must be updated promptly. Any record that is found to be inaccurate beyond alteration, with no link to the offender, should be disposed of regardless of the review type.

Deciding to retain

Reviews of crime or offence-related police information are undertaken in line with the published **schedule**, which determines the length of time between each review dependent on the associated MoPI group. These are referred to as scheduled reviews.

Scheduled reviews require the reviewing officer to conduct an assessment of the risk of harm posed by the nominal under review. This is a two-step process.

Firstly, force decision-makers must use their discretion and take into account all of the circumstances of a case, including the characteristics of the nominal.

If, having considered all the circumstances and the characteristics, the nominal under review meets any of the criteria outlined in the NRAC, the retention of records relating to them is proportionate to the level and type of risk they pose. These records must, therefore, be retained and reviewed again at a later date in line with the review schedule.

Where police information is contained within other unrelated material – for example, police pocket notebooks – the relevant extracts should be included within the appropriate record. Likewise,

executive meeting minutes relating to the governance of a criminal investigation should be incorporated in the relevant case file. Any remaining information within the notebook should be managed in line with the MoPI guidelines or the NRS.

A decision to retain records relating to a particular individual does not necessarily mean that every piece of information held in relation to them needs to be kept. The reviewing officer should use their discretion to identify those records and evidential material that contain sufficient information to contribute to understanding the nature of the offence or the type of risk posed.

Extent of retention

During an investigation, a number of pieces of information are collected for purely administrative purposes – for example, court availability – and do not have any independent significance. It is not necessary to keep these ancillary records as part of a file that has been marked for retention, as they do not contribute to understanding the nature of the offence or the type of risk posed.

Information that is duplicated across force systems should also be minimised. Consideration should be given to the amount and type of detail held on individual systems and the extent to which this is duplicated in others, with a view to disposing of those that are surplus to requirements. It is also more practical to retain electronic records rather than paper ones, although care should be taken to guard against data obsolescence when records are to be retained for long periods.

The paper records can be destroyed provided that the reviewing officer is satisfied that:

- the relevant information contained in paper records is also held electronically
- evidential standards and requirements are met
- the information is available in a searchable format

Original physical exhibits **do not need to be retained** where it is unreasonable to do so. However, a copy should be stored in the form of photographs, video recordings or digital images, in accordance with the Police and Criminal Evidence Act (PACE) 1984 s 22.

The General Data Protection Regulation (GDPR) and DPA 2018 specifically allow the retention of records beyond the period needed for policing or organisational purposes for the purpose of:

- archiving in the public interest

- scientific or historical research purposes
- statistical purposes

Section 41 of DPA 2018 and **GDPR Article 89** detail when the processing of information for these purposes is not permitted.

National retention assessment criteria

The NRAC asks a series of questions focused on potential risk factors, in an effort to draw reasonable conclusions about the risk of harm presented by nominals. Wherever a record is assessed as being necessary and proportionate to the purpose it serves, it can be retained. These questions are as follows.

- Is there evidence of a capacity to inflict serious harm?
- Are there any concerns in relation to children or vulnerable adults? (Where 'concerns' refer to concerns for safety)
- Did the behaviour involve a breach of trust?
- Is there evidence of established links or associations which might increase the risk of harm?
- Are there concerns in relation to substance misuse?
- Are there concerns that an individual’s mental state might exacerbate risk?
- Are there any other issues that impact on the level of risk the individual presents?
- Could this individual be of interest to ongoing public inquiries?

Where the answer to any of the questions is ‘yes’, the characteristics of the nominal and their fundamental rights must be fully considered and balanced against any risk identified during the completion of the NRAC. If, having carried out the balancing exercise, the information relating to the nominal being assessed should be retained, it must be reviewed again at intervals designated by the review schedule, ensuring that:

- records remain adequate and up to date
- records meet national quality standards
- new information can be considered
- risks are still current

A completed copy of this assessment template should be kept on file as a record that the review has taken place and to support the subsequent decision.

An NRAC template should be completed and stored. These can be populated electronically and should be linked to the nominal record.

The key points to consider when completing the NRAC are as follows.

- The infringement of an individual's privacy caused by retaining their personal information must satisfy the proportionality test.
- Records that are accurate, relevant, up to date and necessary for policing purposes are held for the minimum period designated by the appropriate MoPI group. This helps to ensure that forces have sufficient information to identify offending patterns over time, and to guard against individuals' efforts to avoid detection for lengthy periods.
- Beyond the designated periods, there is a requirement to review whether it is still necessary to keep the record for a policing purpose. The review process specifies that forces may retain records related to offending behaviour only for as long as they are necessary, and in accordance with the respective MoPI grouping. The NRAC template provides guidance on establishing whether or not information is still needed for a policing purpose.

Review process

There are three types of review – initial, scheduled and triggered.

Initial review

The initial review of police information will be conducted when the record is created. The information will 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.

The initial review should also identify any MoPI group 3 records that should be taken out of 'deletion without manual review'.

Scheduled reviews

As stated above, reviews of crime-related police information are undertaken in line with the published schedule, which determines the length of time between each review dependent on the associated MoPI group.

Under the review schedule, information held for policing purposes is divided into three MoPI groups. The Police National Legal Database (PNLD) has been updated to show a MoPI review group for each offence. All forces should have access to the comprehensive and regularly updated PNLD list, allowing them to search by offence, offence code and MoPI review group.

When an nominal – for example, no further action, arrested, acquitted or charged – is recorded as MoPI group 3 on a force system, they present as lower risk due to the type of offence(s) they are linked to. A force can decide whether to delete these without manual review (after a six-year clear period) or review them. It is not necessary to review national systems such as the PNC and the Police National Database (PND), although a force may wish to do so if there is evidence of cross-border activity.

If a force does choose to delete group 3 records without manual review, they should put in place mechanisms to identify, at the point of initial review, any records that should be excluded from that process. This should be for offences that, although group 3, may be seen as a precursor to more serious offending. The chief officer must also be confident that data quality is sufficient for automated decision making.

However, due to the potential risk of group 1 and 2 nominals to commit serious sexual or violent offences, consideration must be given to the national record and the review must include a PNC and PND check.

If a group 1 or 2 nominal is found to have committed, or is suspected of committing, a group 3 offence in another force area, the review should consider whether this changes the level of risk posed by the subject when making the decision whether to retain or delete. If the decision is to retain, then the clear period should be reset.

Scheduled reviews also apply to potentially dangerous people who have not yet been convicted or even accused of serious offending but whose behaviour nonetheless causes concern, for example, individuals identified by intelligence reports.

Designated clear periods prevent forces from having to justify the continued retention of information related to prolific offenders for as long as they continue to offend.

Where victims and/or witnesses are linked to the records being reviewed, consideration needs to be given to the continued retention of their details. It will, on most occasions, be proportionate and

necessary to retain details of victims and witnesses for the completeness of the data. Forces should have processes in place for considering deleting such information if a request for deletion is received. It is a legal requirement under DPA 2018 that forces have processes in place to deal with all requests for erasure. This applies to offenders, victims and witnesses.

The review schedule focuses on the nominal rather than on business areas. It is based on the following four premises.

- Past behaviour is an indicator of future behaviour and the type of offence an individual is involved in, or alleged to be involved in, is a clear indicator of risk.
- Information relating to those offenders who pose the highest risk of harm to the community must be retained the longest.
- Where a person record is linked to multiple offences, the most serious offence determines the review category for all of the offences.
- A clear period has been reached, in that there has been a sufficient period of inactivity on the record.

When undertaking a scheduled review, the presumption should be that the record is deleted unless a reason is found that justifies retention. The justification will be based on the risk that the nominal continues to present. Forces should determine the extent of their scheduled reviews but they may wish to include the following.

- Duplicate records are identified, matched, merged and deleted where appropriate – all local systems (live and legacy should be checked for duplicate records).
- Key nominal data is adequate, relevant and not excessive.
- The highest MoPI grade is identified for all pieces of information.
- Links and associations that are reflective of the information are included.
- Address and vehicles history (where appropriate) were accurate at the time the record was created.
- Information is assessed to determine any relationship to current independent inquiries.
- Forces have adequate processes in place to enable reviewers to identify records that need to be retained locally and these processes are robust and followed.
- Data has been considered to understand the relationship between the nominal and the information under review to determine retention (for example, victim, witness, suspect or offender).

If no other justification for retention can be found, the PNC and PND must be checked when reviewing MoPI group 1 and 2 nominals. This will not be routinely required in MoPI group 3 cases. The PNC and PND checks are particularly important in the cases of:

- potentially dangerous persons and public protection matters
- local intelligence that suggests travelling criminality

Where additional information is found, forces should take into account clear periods and risk to determine further retention of information, making use of the NRAC.

Triggered reviews

A triggered review provides the ability for forces to review a nominal record where appropriate outside of the normal scheduled review process. There are three types of triggers for a manual review, as follows.

Information added of a higher MoPI group

New information is added to the record of a nominal that is of a MoPI group higher than the one already recorded against them. The record should reflect the new MoPI group across all pieces of information. This may be automated where possible.

As a minimum, this type of triggered review should ensure that the highest MoPI group recorded is accurate, establishing the correct retention period. If a manual review is undertaken, related information that is contained within a person's record and is no longer necessary for a policing purpose should be disposed of. Any record that is found to be inaccurate must be updated.
A record found to be inaccurate beyond alteration should be disposed of.

By the time a review is triggered, the information under review may have already been used to make decisions and justify police action. Consequently, any updates must be adequately documented for audit purposes. A triggered review initiated by new information will reset the clear period.

Concerns about adequacy, relevance or accuracy

There are concerns about the adequacy, relevance or accuracy of a record that have surfaced during, for example, **Disclosure and Barring Service (DBS)** checks, FOI checks, subject access requests or requests for deletion of information.

Forces should have mechanisms in place that allow triggered reviews when there are concerns about the quality of information contained within the record. This provides the opportunity to consider resolution of significant data quality issues or to deal with requests for deletion from members of the public that have been approved by the chief constable or relevant delegated chief officer. Manually generated reviews may be undertaken at any point during the lifecycle of the data held and as many times as necessary to ensure that the data is accurate, is relevant and meets a policing purpose.

When disclosing information as a result of DBS checks, FOI requests, subject access requests, or sharing data between forces or with partner agencies, those responsible should be mindful of the accuracy of the data they are disclosing. Basic checks should be conducted prior to disclosure to ensure that the information being provided is accurate, relevant and of sufficient quality. Subject to requirements, any significant issues identified should instigate a triggered review of the record and any updates must be adequately documented for audit purposes. A manual review to address data quality issues of this nature would not reset the clear period.

Deceased nominals

If credible information is received that a subject has died, then a review can be triggered or the force can wait until the next scheduled review. Considerations regarding deleting the record are at **s 4.1**.

The policy for completing triggered and manual reviews in each force should be published and clearly communicated to all relevant staff, to ensure understanding and adherence across the organisation.

Management of police information groups

The review schedules (below) apply to information related to people convicted, acquitted, charged, arrested, questioned or implicated with an offence within the relevant group.

Group 1 – certain public protection matters

Each MoPI group is recorded against the offence on the PNLD.

Information relating to subjects in this group may be retained until the subject has reached 100 years of age (calculated using the subject’s date of birth). A decision to delete this information or

otherwise should then be made on the basis of a manual review. This information should be reviewed every ten years to ensure that it is adequate and up to date, and that retention is justified. Some parts of the group 1 nominal record need not be retained if they are not relevant or necessary.

Information retained under this grouping can include intelligence reports of any grade.

Group 2 – other sexual, violent or serious offences

Each MoPI group is recorded against the offence on the PNLD.

Information relating to sexual, violent or serious offences that are not listed as serious specified offences in **Schedule 18 of the Sentencing Act 2020** can be retained only for as long as the offender or suspected offender continues to be assessed as posing a risk of harm, using the NRAC.

After every 10-year clear period, these records should be reviewed and a risk-based decision should be made on whether they should be disposed of or retained.

If the nominal in question continues to offend or is implicated in continued offending, records relating to them must be retained. In these circumstances, however, the resetting of the clear period means that forces do not have to conduct a scheduled review or justify the continued retention of such records.

Group 3 – all other offences

Records relating to people who are convicted, acquitted, charged, arrested, questioned or implicated for offending behaviour that does not fall within group 1 or group 2 are dealt with in group 3.

Group 3 offences may be deleted without manual review, after a six-year clear period, if certain criteria are **met**.

Undetected crimes

Undetected crimes with no named suspects will be retained in line with the relevant MoPI group based on offence type.

Review schedule

The table below gives examples of the offences and record types of information that are included in each group. The PNLD should be used as the source for determining the MoPI group associated with an offence.

Review group	Examples of offences and record type	Action	Rationale
Group 1 – serious offences and public protection matters	Multi-agency public protection arrangements (MAPPA) managed offenders. Offences specified in the Sentencing Act 2020 Schedule 18 which carry a maximum sentence of 10 years or more. Potentially dangerous people.	Having taken into account the retention criteria detailed above, you may retain until the nominal has reached 100 years of age, then carry out a manual review. Review every 10 years to ensure adequacy and necessity.	This category poses the highest possible risk of harm to the public.

Review group	Examples ofoffences and recordtype	Action	Rationale
Group 2 – other sexual and violent offences	Sexual offences listed in Schedule 3 of the Sexual Offences Act 2003. Violent offences specified in the Home Office counting rules for recorded crime and the National Crime Recording Standard. This group also includes offences specified in Schedule 18 of the Sentencing Act 2020 which are not Group 1 offences, ie, carry a maximum sentence of less than 10 years. Other serious offences are recorded as such on the PNLD.	Review after an initial 10-year clear period. If the subject is deemed to pose a high risk of harm, retain and review after a further 10-year clear period.	NRAC.

Review group	Examples ofoffences and recordtype	Action	Rationale
Group 3 – all other offences	All other offences.	Retain for an initial six-year clear period, followed by subsequent five-year clear period reviews. Either review and risk assess after a six-year clear period 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.

Clear periods

The review schedule in the NRAC states that reviews take place after designated clear periods. For the purpose of information management, a clear period is defined as the length of time since a nominal last came to the attention of the criminal justice system as an offender or suspected offender for behaviour that can be considered a relevant risk factor. Where victims and/or witnesses are linked to these events, consideration needs to be given to the continued retention of their details. It is most likely to be proportionate and necessary to retain details of victims and witnesses for the completeness of the data. The nominals will not be assigned a MoPI group but their data will be retained in line with the MoPI group of the record to which they are linked.

A clear period will begin:

- on the date that an intelligence report was submitted
- on the date of the last police action relating to offending or suspected offending behaviour
- when there is an issue date (fixed penalty notice or caution)

- on the date a decision was taken or handed down (either the case is not proceeded with or there is an acquittal)

If the nominal's last relevant contact with the criminal justice system was by way of a court-ordered sentence, the clear period begins when that sentence or any determination that has a time dependency has expired.

For example, when community service has been completed, or in the case of custodial sentences, this includes any period served on licence in the community following the custodial element of the sentence.

Forces should take a pragmatic approach in cases where whole life sentences are imposed in fraud cases, where the perpetrator is required to repay debt over their lifetime. In these cases, a review of six or ten years after sentencing would be appropriate dependent on the relevant MoPI group.

A clear period will be reset when:

- the nominal is arrested
- an outcome is applied (for example, no further action or charged)
- the nominal commits a new offence
- the nominal is suspected of committing a new offence
- there is other evidence that the subject presents a risk of harm to others
- an intelligence report identifies the subject as a person of interest, not a victim or witness
- the nominal has their firearms licence revoked or firearm application refused
- when there is an information request that suggests the nominal is still offending or presents a continued risk
- the nominal is the subject of a DBS disclosure when an intelligence report should be submitted

To automate the process, forces may identify the factors within the information categories described above, which will reset the clear period. Clear periods are not reset by subject access requests.

An information request will not routinely reset a clear period. A reset will be dependent on the nature of the information request. The recipient of the request should make the decision based on whether the request indicates new information relating to the level of risk presented by the subject.

Documenting the review process

In the case of a scheduled review, the NRAC template should be completed and stored either electronically or in hard copy in the relevant file.

The retention assessment criteria section of the NRAC template determines whether or not the information under review should be retained or disposed of. This section must be used for all scheduled reviews. The reviewing officer must include an explanation on how the individual in question meets the outlined risk criteria. It is not necessary to explain how or why an individual does not meet the risk criteria if this is the case.

If the NRAC template is being used, the outcome of the review section must always be completed and must include an explanation of any decision to retain or delete. Any other changes to the record should be auditable either by manual recording on the template or by the IT system automatically logging changes.

A record should also be kept of every triggered review. Any system-generated records created to document a review must log the date of review, the reviewer's name, the outcome and the reason for the decision taken, linked to the NRAC. In complex cases where the review process takes several days, a time period can be recorded as the date of review. For triggered reviews, the reviewing officer must provide an explanation of how and why the triggered review was initiated.

Deletion of records without manual review

Any deletion of MoPI group 3 records without manual review must be predicated on good data quality. The force would need to satisfy themselves that the necessary data quality checks and balances are in place, and that quality is sufficient to allow for what is essentially a technical review. There would need to be some rules attached to this.

- Forces must have taken a risk-based approach and ensured their decision is documented and authorised.
- There must have been a minimum clear period of six years.
- Forces' systems would need to be able to automatically review the full record of a person to determine they fit the criteria.

Forces may wish to build in additional safeguards whereby categories of group 3 records, normally the subject of deletion without manual review, are taken out of this process. This may be by flagging records during the initial review, or through the automatic identification of words or phrases that may be an indicator of a heightened level of risk, such as the offender may be grooming or exploiting the victim.

Forces should not consider the deletion without manual review option for group 1 or 2 offences.

Disposal

The key points to consider when a decision is made to dispose of information after a scheduled review has taken place are:

- no details of the record should be retained, other than that identified as required for audit purposes
- as a minimum, personal information relating to the records should be pseudonymised so that no living individual can be identified
- the information is disposed of securely
- audit arrangements are in place to quality control a random sample of decisions
- reviewers should ensure that information to be disposed of is not duplicated and retained elsewhere

Disposal means removal of information from all local police systems and in all data formats, justified through the review process, to the extent that it cannot be restored. This includes paper copies or those within other documentation, such as intelligence products. Local force policy should set out who can authorise the disposal of police records.

Information must be disposed of in accordance with information assurance guidance and GSC. All forces must develop and implement a policy for disposing of records in accordance with the above.

Deceased persons

When a nominal is known to be deceased, it is proportionate to consider the disposal of records relating to that person. This can be completed at the next scheduled review or as a triggered review where all of the following criteria are met.

- Clear documented evidence that the offender has died and how the offender has died.
- Consideration should be made to any potential investigation under certain circumstances, such as historical sexual offences.
- The offender or suspect has offended alone. If not, consider a clear period.
- The clear period for any additional persons has been met. The clear period is determined by the MoPI offence category for each additional person if there are more than one. Retention is determined by the aggregated MoPI category for the individual(s) and not the MoPI category for the event that links the offenders together.
- The impact on the living (victim) has been considered.
- There is a single victim. Where there are multiple victims, this increases the potential for additional victims following charge and, as such, further retention of material relating to the offender should be considered.
- If a nominal dies during a police investigation and before a formal charge has been brought, it may be appropriate to retain information. This would be if lines of enquiry lead away from the original suspect to another suspect, or if the offence was committed by just one person, there was a single victim and there is overwhelming evidence against the deceased. The force should ensure that any retention includes the appropriate timescales for a victim's right to review.
- The person, or the crime and intelligence linked to the deceased person and any additional people, is not relevant to any ongoing relevant independent enquiry.
  - Under **the Inquiries Act 2005 s 21**, an inquiry has the power to order the production of documents. Failure to comply with such an order without reasonable grounds is potentially an offence punishable by imprisonment.
  - It is also an offence for a person to destroy, alter or tamper with evidence during the course of an inquiry that may be relevant to that inquiry, or to deliberately act with the intention of suppressing evidence by preventing it being disclosed to the inquiry.
  - Institutions have an obligation to preserve relevant records for an inquiry for as long as necessary to assist that inquiry.
  - The obligation to retain documents will remain throughout the duration of an inquiry, to ensure that evidence is secured.
- The records should be archived because they are of historical significance or of public interest.

If the decision is made not to delete the record, after consideration of the criteria above, then a new review should be scheduled using an appropriate time scale dependent on the nature of the issues

identified.

Audit and supervision

Forces should document the level at which decisions to dispose of records relating to sexual, violent and serious offences are taken and any authorisation needed.

An audit should be undertaken based on a clear understanding of the data protection and Police information and records management Code of Practice principles.

In cases where a record has been marked for disposal, it is not appropriate to retain the completed NRAC template for audit purposes, as this contains details of the record and undermines the attempt to remove this from police systems. The force should ensure that a disposal schedule is maintained containing the following information.

- Date of decision.
- Number of records.
- Whether the records were considered inadequate or no longer necessary for a policing purpose.

Records documenting a decision to dispose of information should not, under any circumstances, hold the personal details of individuals. Forces should follow the review process to ensure that they can justify the disposal of information. Once a record is considered to be either inadequate or no longer necessary, there should be no indication that the force ever had it. However, to facilitate audit, it may be necessary to keep a copy of a proportion of the records deleted, perhaps by taking screenshots, for up to one year.

In order to ascertain compliance, forces should undertake regular MoPI compliance tests. These have been developed to reflect the key principles of MoPI, the requirements of the APP on Information management and data protection principles.

Legacy data

Not all forces make the decision to migrate data from one system to another. If this is the case, then it is important that any relevant legacy data is captured as part of any review, retention and disposal process. Legacy data is defined as information stored in an old or obsolete format or computer system that is difficult to access or process, or is no longer added to. Any data held on a

legacy system will need to be managed to ensure that it complies with data protection principles and the APP on Information management.

Prior to assessing legacy data, forces should consider the following to allow risk-based decisions to be made about the retention of the data:

- The purpose of the system and whether the business process is still current.
- When the system was live and whether any elements within it are still being updated.
- Any links between the legacy data and existing systems.
- Whether the data is searchable.
- What data was migrated, if any.
- Volumetric data analysis – for example, date parameters, entities, data purpose.
- The profile of the data and the risks linked to it.
- Data retained in relation to any ongoing public inquiry.
- Digital continuity.
- Whether the record meets the criteria for permanent retention.

All decisions to manage legacy data should be signed off by the SIRO. This could include bulk deletion or data migration. Forces who choose not to manage legacy data must understand and document the risk inherent in this decision.

Decisions to delete could include:

- data that has been migrated across to subsequent systems and is therefore duplicated within the legacy system
- data that is not person-centric (names contained within free-text fields) and may therefore offer little operational value, and the search capability is limited
- data that is no longer readable or useable
- poor-quality data

Cancelled crimes

Upon investigation, a report of a crime may be cancelled. This can normally only take place where the following apply and is authorised by the force crime registrar:

- additional verifiable information that becomes available determines that no notifiable crime occurred
- the crime was committed outside the jurisdiction of the police force in which it was recorded and there is evidence that it has been recorded by the other force
- it is a duplicate record or part of a crime already recorded
- the crime was recorded in error
- it is self-defence claimed (for specific recorded assaults)

Cancelled crime records should be assigned to the MoPI group appropriate for the substantive offence. The record should be reviewed after six years for group 3 or after ten years for groups 1 and 2, provided there had been the requisite clear period for the nominal identified on the cancelled crime. Group 3 may be deleted without manual review but groups 1 and 2 should still be subject to a manual review. If any cancelled crime is subject to a triggered review, for any reason, then a decision may be made to delete at that point irrespective of the MoPI group, provided the record is more than six years old.

Similarly, if an incident is recorded that alleges behaviour that falls short of the course of conduct that would trigger a substantive offence, then the record should be assigned to the MoPI group for that offence (for example, a hate crime incident). This will give forces sufficient time to evaluate whether this incident is part of an ongoing course of conduct that would lead to the offence being committed.

Other police purpose and corporate information and records

Retention periods for all police information that is not related to criminal or alleged criminal behaviour will be included in the NRS. Forces may wish to build on the minimum retention periods in the NRS to create their own retention schedule, to represent the nature of the records and information assets created by the force.

Other police purpose information is obtained or recorded for a police purpose that is not related to crime or offending behaviour, such as missing people, lost and found property, licensing records, event notifications and road traffic collisions (where there is no indication or suspicion of offending behaviour).

Guidance on the retention of these records can be found in the **NPCC National Retention Schedule (NRS)** (currently under development). You will need to log in to the Knowledge Hub.

Other policing purpose and corporate information and records can be deleted without review at the end of the designated retention period. However, forces should build the ability to identify records that should be reviewed before deletion, or where the designated retention period should be extended, into their IT systems.

This might include the use of qualifying or closure codes in incident report records or the use of flags when records are created.

Deletion of records from national police systems ('Record Deletion Process')

The review, retention and deletion process as described in this APP and the Police information and records management Code of Practice does not apply to the deletion of information and records held on the PNC.

An individual can, however, make an application for record deletion under the NPCC Record Deletion Process (RDP), which is managed by Information Management at ACRO Criminal Records Office. However, this does not apply to court convictions. Forces should not remove these from the PNC unless they are incorrect or authorised by the Secretary of State, such as disregarded offences and court orders.

The RDP is outlined in the guidance **'Deletion of Records from National Police Systems (PNC/NDNAD/IDENT1)'**.

Custody images

This APP supports the **Home Office (2017) Review of the Use and Retention of Custody Images**.

Custody image management should be in line with the review schedule for MoPI groups. An individual can apply to chief officers to request deletion of their custody image.

The individual may request deletion where they were:

- arrested but not charged
- not convicted of the offence for which the image was taken
- convicted and a predetermined time (group 3 deletion) has elapsed since the conviction

Where an individual who was not convicted makes an application, there should be a presumption in favour of deletion. Chief officers have the discretion to retain a custody image where this is necessary for a law enforcement purpose and there is an exceptional reason to do so. Examples might include where the individual is considered to pose a substantial risk of harm when assessed against NRAC.

Forces should ensure that the process for making an image deletion application is clear and transparent. They should include information about the right to have images deleted and other information requests on the force website.

Where a formal request for deletion is not made, the image should be managed in line with this APP information management review schedule.

Request for deletion

Individuals have the right to apply to chief officers to have all or part of their records erased. A request will trigger a review under the MoPI principles. However, this section deals specifically with the request for erasure of a custody image.

Accepting a request for deletion

Individuals have the right to apply to chief officers to have their **custody image deleted**. Individuals applying for deletion of custody images must produce suitable identification to allow the processing of their personal information and to determine they are the data subject. This must be photographic identification, such as a passport or photographic driving licence, and proof of address, such as a council tax or bank statement.

Identification materials should be deleted once the decision to retain or dispose is reached.

Individuals arrested but not charged, or charged but not convicted, have the right to request deletion earlier than those timescales set out by the APP on Information management. Only images that relate to the offence that removal has been requested for should be taken into account. Previous or subsequent images for convictions or arrests should not be considered, unless they

form part of the general review process.

Images held in relation to custody that have been requested to be removed in the application will be the only images considered as part of the process. An application must relate to a specific arrest or event that led to the taking of the custody photograph. Each arrest or event requires a separate application.

It is important to check for multiple copies of the custody photograph subject to the application and ensure that these are all deleted as well. Copies may be held in both local and national systems.

Where custody photographs are deleted, a system record needs to be completed to show that a custody photo has been disposed of. The date of deletion and who authorised it should be recorded for audit and completeness.

Image information

Understanding the level of risk associated with continued retention and bulk deletion of custody images is important. The overall risk is determined by the force risk appetite.

The following considerations will help forces gain a better understanding of the image and the offender or suspect.

- Age of the offender or suspect at the time the image was taken.
- Nature of the offence for which the specific image was taken.
- The date when the image was taken.
- The number of images relating to a single person and the timeliness of these images.

There is less risk of deleting images older than six years for people under the age of 18 arrested for a MoPI group 3 offence, irrespective of outcome.

Custody image review

When a custody image is reviewed either by triggered or scheduled review, consideration on retention must include:

- whether the image meets the national standard on size
- resolution

- how well it identifies the person (quality)

Decision making

Where an application for deletion is made, forces should use the NRAC to review whether the custody image should continue to be retained, regardless of the MoPI group. The NRAC questions will:

- support forces in identifying any risk posed by the individual and will ensure that any decision to retain or dispose is based on known evidence and intelligence
- provide the necessary audit trail for any possible subsequent appeal and complaints to the Information Commissioner's Office
- ensure consistency in decision making locally and nationally

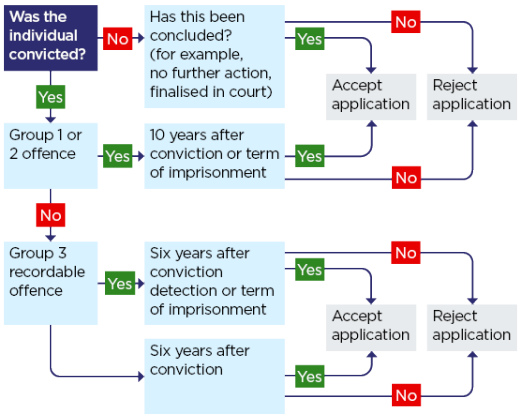
Police presumption criteria

When reviewing images with a view to deleting, consider the following.

<table>
<tr><th>Applicant</th><th>Presumption of deletion</th></tr>
<tr><td>Adult convicted of a recordable offence</td><td>No presumption in favour of deletion.</td></tr>
<tr><td>Adult convicted of a non-recordable offence.</td><td rowspan="3">Presumption in favour of deletion.</td></tr>
<tr><td>Adult arrested for but not convicted of a recordable offence.</td></tr>
<tr><td>Under 18 convicted of a recordable offence.</td></tr>
<tr><td>Under 18 convicted of a non-recordable offence.</td><td rowspan="2">Strong presumption in favour of deletion.</td></tr>
<tr><td>Under 18 arrested but not convicted of an offence.</td></tr>
</table>

Accepting a request for deletion

The following diagram outlines the requirements that need to be met to process a deletion request.



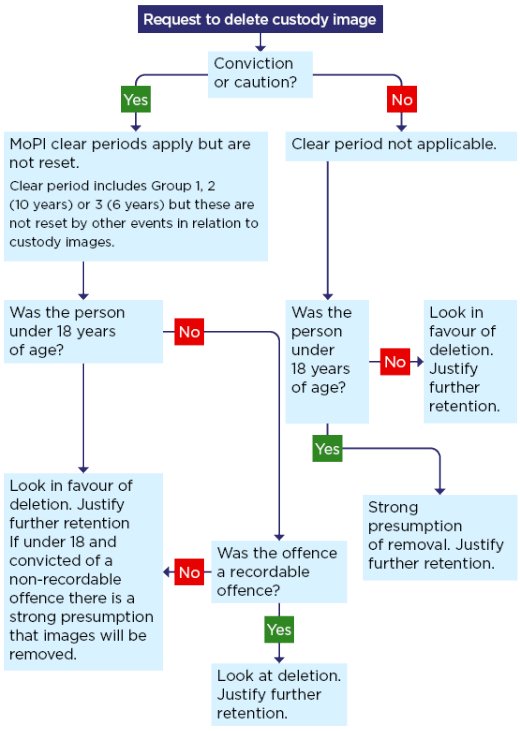
Where any of the above criteria are not met, the applicant should be informed and updated on when they can make a further application for removal.

Managing the process

Forces have the ability to retain an image if there is clear and evidenced risk. Forces must be able to justify continued retention and not attempt to justify deletion. This process should be documented using the NRAC.

Where the police presumption criteria for accepting the request have been met, the flowchart below should be considered when dealing with and managing the request.

The following diagram outlines the requirements that need to be met to manage the process.



Responding to applicants

Where deletion of a custody image or photo has taken place, the applicant must be informed. If this is part of the normal review process and a decision to delete is made, the person does not need to be informed. All NRACs can be requested under the subject access procedure, subject to certain exceptions as below.

Where the decision is to refuse deletion, the applicant should be informed of:

- the reasons for refusing deletion, unless there is a compelling reason not to do so, for example, ongoing investigation or intelligence that is not to be disclosed
- the date of the next review schedule
- the date when the applicant can reapply for deletion

Templates

When responding to an applicant who is requesting an image deletion, the following templates should be used:

- **letter for confirming disposal**

- **letter for refusing disposal (criteria not met)**
- **letter for refusing disposal (can disclose)**

Archiving of records in the public interest

This APP relates to records that are being considered or have been selected for permanent archiving, not those still within operational use.

Preservation of records in the public interest

Certain police records should be archived for their historical value and enduring public interest, or for academic, scientific or statistical purposes. This category may apply to records in all formats that:

- are beyond their required retention periods
- have reached the end of their business life
- have no further business, legal or regulatory use

A justification is required for keeping records permanently.

Chief officers should appoint an individual(s) or role holder(s) to be responsible for information and records management, including archiving and access. It is important that those responsible should make themselves familiar with their responsibilities under the following Codes of Practice.

- **Code issued under Section 46 of the Freedom of Information Act (FOIA) 2000**
- **Police information and records management Code of Practice**

Throughout this authorised professional practice (APP), a reference is made to forces having to take an action. This is because it's likely that decision making will be undertaken by a variety of people in different roles, due to the different ways forces are structured. Chief constables need to make arrangements to ensure that it's clear which person is responsible for each decision set out in this guidance.

Processing of archived records

Some information archived by forces may contain personal data. In these circumstances, chief officers must ensure that their force complies with the appropriate data protection requirements and

safeguards for archiving in the public interest, as set out under both:

- the General Data Protection Regulation (UK GDPR)
- Part 3 of the Data Protection Act (DPA) 2018

See the National Archives website for further detail of the legal framework regarding the archiving of records.

Under **Part 3 of the DPA 2018 s36**, when archiving records that contain personal data, **controllers** need a specific authorisation in law beyond their law enforcement purposes. This can include clear common law tasks, functions or powers (including implied powers), as well as those set out in statute or statutory guidance (including a statutory code).

The power to authorise is provided by **Principle 7 of the Police information and records management Code of Practice**. This underpins consistency in the way that forces archive records in the public interest.

Assessment and preservation criteria

Chief officers should ensure that their force has systems and processes in place to identify records that meet the criteria for permanent preservation. Early identification of such records is beneficial. Information concerning proposed permanent retention for archiving of some classes of records should be recorded on a force's retention schedule.

However, there is an ongoing need for assessment throughout the life of records, as their significance changes over time and may not be obvious at an early stage.

The expiry of the operational retention period for the identified record(s) – as determined by the **National Police Chiefs' Council (NPCC) Forces' Retention Schedule** or the **Information management APP** – provides an opportunity for the collection to be reviewed in its entirety. At this point one of the following decisions should be made.

- Keep all contents.
- Keep selected contents.
- Dispose of all content.

Chief officers should ensure that their force documents why certain records or categories of records are selected for permanent preservation. Forces should also be able to explain why information is no longer held, either by reference to a record of its destruction or to its policy as recorded in its retention schedule.

When archiving in the public interest, forces must make sure that technical and organisational measures are in place to ensure respect for the principles of data minimisation under **article 89(1) of the UK GDPR**. This involves selecting and retaining the minimum amount of personal data that is required to preserve the integrity, authenticity, context and historical value of the record.

Normally, a collection of records will be considered by records managers for permanent preservation, rather than individual records (although individual records can be selected). It is important to consider paper and digital collections, as well as other mediums, such as microfiche, photographs, audio or visual records.

Most types of records will include **special category and criminal offence data**, which are given greater protection under UK GDPR. In those cases, records managers must take particular care to record why, for each type of record, the interests or fundamental rights and freedoms of the data subject are overridden by the public interest in archiving these records. It is advisable, and sometimes a requirement, to carry out a Data Protection Impact Assessment (DPIA). The DPIA can identify and minimise the risks of archiving records containing special category and criminal offence data.

Chief officers should ensure that their force seeks to preserve records that:

- relate to a crime or incident of significant local or national interest, including supporting minutes of ‘Gold Group’ meetings
- demonstrate major changes to the force
- capture something of significance happening for the first time
- reflect changes in attitudes, policies and strategies
- promote or document issues unique to the force
- provide evidence of major projects, functions or activities
- describe governance arrangements, a high-level decision-making process or a specific decision
- contain material that reflects the views or activities of individuals who have played a significant role in the development of the forces

- possess aesthetic qualities and/or would be valuable for exhibition or academic research

The **NPCC retention schedule** (you will need to log in to Knowledge hub) gives further details about the categories of document that should or may be considered for retention.

Outside the criteria above, forces may choose to permanently preserve specimens of records – such as minor crime files or custody records – to illustrate how crime investigation has evolved for future generations.

Forces may also decide to permanently preserve a class of record – such as details of persons employed by forces – which may be of historic interest.

Safeguards

Section 41 of the DPA 2018 sets out the safeguards for archiving records, containing personal data, under Part 3 law enforcement purposes. **Article 89(1)** and **Part 2, section 19 of the DPA 2018** sets out the safeguards for UK GDPR.

Archiving information that contains personal data in the public interest is only permitted if the processing:

- is not carried out in connection with measures or decisions in relation to individual data subjects
- is not likely to cause substantial damage or substantial distress to a data subject

Archive arrangements

Forces should have arrangements in place to archive records that are no longer required for a policing or organisational purpose and which have been selected for permanent preservation, in line with the **assessment and preservation criteria**.

Permanently preserved records may be kept at:

- a force location (archive or police museum)
- an external storage provider
- an external archive (where records can be made available for research purposes), subject to local agreement

Where historic records that contain personal data are held externally, forces must comply with Article 5(1)(f) of the UK GDPR. This ensures that technical and organisational measures and infrastructure are in place to ensure the confidentiality, integrity and availability of systems and services, as well as the personal data processed within them.

The provider should have storage conditions that conform to relevant standards, such as those issued by the British Standards Institute.

- **Collections Trust – BS EN 16893:2018 Conservation of Cultural Heritage**
- **National Archives – Caring for archives**

If the force intends to preserve the records itself, it should comply with these standards.

In the case of digital records, care must be taken to ensure long-term accessibility. In some cases, it may be necessary to migrate records to newer formats or systems to maintain accessibility. Equal consideration should be given to maintaining metadata, as well as avoiding quality and data loss.

Continuity of records and metadata must be considered whenever new systems are implemented and data is migrated from **legacy systems**.

Migration exercises provide an opportunity for records within redundant legacy systems to be identified for permanent preservation and transferred to an archive, instead of being moved to the new system alongside information still needed for business use.

When a force archives records in-house, the force should ensure that an identified individual is responsible for managing the archive. This should include the preservation of (including digital preservation), storage of, access to and cataloguing of the materials. A recovery plan should be put in place to protect and recover the archive in the event of a disaster.

If forces make arrangements with an external storage provider (as opposed to an external archive service), the force will retain responsibility for:

- decisions about access arrangements, including decisions about disclosing any elements of records that are subject to FOIA exemptions and undertaking the necessary redaction
- decisions about information rights requests under UK GDPR
- the records overall, ensuring that the conditions and terms of contract are maintained

- ensuring that all records remain accounted for
- making sure that there is an audit of the movement of files and boxes in and out of the store, as well as who has requested access and why

Forces should consider retaining particularly sensitive records in their own archive stores until the sensitivity has sufficiently diminished.

Details of accredited archive services in the United Kingdom are available on the **National Archives website**. Local authority archive services are empowered to accept records of local significance under the Local Government (Records) Act 1962.

If transferring records to an external archive, consideration needs to be given to the terms and conditions of the transfer. This will have an impact on the roles and responsibilities of both the force and the external archive following transfer. These terms and conditions should be agreed between the force and the archive and recorded in a deposit agreement.

A deposit agreement should detail:

- who has data controller responsibilities or if they are shared
- who will manage information access requests, including who is responsible for making disclosure and redaction decisions
- how records will be transferred
- how this will be recorded by the force
- any processes for the force to recall the records

External archives are able to accept material with a protective marking of official-sensitive or below.

Forces should keep a schedule of records that are permanently archived, either in-house or externally (with an external storage provider or an external archive). This should include:

- detail relating to the nature of the record (including any metadata required to make the records searchable, such as named individuals or topics)
- the start and end date of any records in a collection
- their security classification
- any FOIA exemptions applied and the review periods for such exemptions
- their context and location

Ownership

External archive services may accept transfers of records as an outright gift, where ownership of the records transfers to the archive service. Alternatively, external archive services may accept transfers of records on loan. This is sometimes known as ‘on deposit’ or ‘indefinite loan’.

The external archive will be able to discuss the implications of each option with the force, and will normally be able to share their standard terms and conditions of deposit forms to help inform the decision.

- Gift – the records are no longer the property of the force. They cannot be withdrawn at a later date and the force is no longer involved in decision-making about the management or administration of the records.
- Loan – the force retains the ownership of the records. Subject to negotiation with the external archive, the force may be able to withdraw the records at a later date and develop a collaborative relationship with the external archive, with respect to the ongoing management or administration of the records. The external archive may request a contribution towards their costs, such as storage boxes and removal costs.

Access decisions

When determining whether the records are to be transferred as a gift or a loan, consideration needs to be given to the process by which decisions will be made about access to information held in the records following their transfer to the external archive.

If records are transferred as a gift, FOI and data controller responsibilities will transfer to the external archive.

If records are transferred as a loan, the force and the external archive have the opportunity to agree an access decision framework. This allows both parties to determine in advance how requests for access will be managed, and allows for consultation with the force as the record creator in specific, defined circumstances.

Where there is a request for information that has previously been transferred with exemptions or exceptions, the archive should consult with the force prior to disclosure. The force will be responsible for reviewing the information for any remaining exempt information and for making any further representations as to why it should be withheld.

Before public access to records is allowed, consider aligning the release of sensitive information with other law enforcement partners who have interest and/or equity in the records. It is strongly advised that consultation is undertaken to avoid inconsistent and conflicting releases of records. The National Crime Agency (NCA) and its precursor agencies are of particular consideration. Information received from, or relating to, the NCA is exempt information under section 23 (national security) of the FOIA.

The NCA should always be consulted before information is made available to the public. Particular care should also be taken where the NCA, or any of its precursor agencies, are involved due to their responsibilities under the Public Records Act 1958 to select records of historical interest for preservation at The National Archives.

Access arrangements

Prior to transferring records to an external archive with public access, forces should perform a sensitivity review of the records, in order to determine their access status. National Archives have published a **Sensitivity review: Quick reference guide**. Although not police-specific, this provides useful guidance on carrying out a review.

Before transferring records to an external archive, the following will need to be considered.

- Whether the records will be transferred open, with public access permitted.
- Whether part or all of the record contains sensitivities, in which case public access may need to be restricted. Forces must identify appropriate exemptions under FOIA and the Environmental Information Regulations 2004 (EIR) for information that remains sensitive, to ensure that public access is restricted to all or part of the record for an appropriate period of time. If applying an exemption, the force should:
  - identify the information clearly
  - cite the relevant exemption(s) engaged by the record
  - explain why the information should not be released
  - identify a date at which either release would be appropriate or the case for release should be reconsidered

Original records must be preserved in order to protect their integrity. Only copies of records can be redacted for access or other purposes.

Records containing the details of confidential informants (sometimes referred to as covert human intelligence sources (CHIS)) are not considered suitable for eventual public access. The appropriate FOIA exemptions should therefore be applied and the force should consider keeping them in-house. Other records that are initially deemed unsuitable may become suitable after a lengthy time period has passed.

If a force needs to review its own records that are held in an external archive, wherever practical they should review the records onsite at the archive and/or make their own copies. The originals should remain in the archive unless there are exceptional circumstances that make onsite review untenable or unreasonable.

Records that leave the archive must be properly documented, as the force will hold the information and will be required to meet its obligations under FOI and data protection legislation. Forces have the option to pay for copies of the records deposited in the archive.

However, where a force removes copies, they will also hold that information for FOIA purposes. Any FOI responses should be shared with the archive to ensure consistency of access. If records are removed, their timely return to the archive should be a priority.

If a large volume of records is required, reviewing them in smaller batches should be considered in order to expedite their return.

Summary

In summary, force archiving arrangements, whether in-house or external, must include:

- a schedule of permanently archived records, as well as their location
- arrangements that keep collections, in all formats, safe and accessible
- arrangements for managing FOIA requests
- adherence to the DPA 2018 and UK GDPR, where records contain personal data
- resource commitments (people, facilities, finance, IT) necessary to maintain the arrangements
- coherent policies, plans and procedures
- an appraisal, selection and sensitivity review process
- arrangements that build in data protection legislation safeguards, including completion of a DPIA where the archiving is likely to result in a high risk to the rights and freedoms of individuals
- a disaster recovery plan

Tags

Information management