Records Management
POLICY & PROCEDURE

OFFICIAL

Government Security Classification Scheme	*Policy section:* **OFFICIAL - Force website approved** *Procedure section:* **OFFICIAL - Force website approved**
Department of Origin	Criminal Justice
Policy Holder	Chief Supt, Head of CJ
Policy Author	Records Manager
Related Information	Review, Retention & Disposal; Records Management Policy & Procedure Data Protection Act 2018 Freedom of Information Act 2000 Protection of Freedoms Act 2012 Lord Chancellor's (2009) Code of Practice on the Management of Records Issued under Section 46 of the Freedom of Information Act 2000 Data Protection Policy & Procedure Government Security Classification Scheme Policy & Procedure Information Security Policy & Procedure College of Policing Information Management Authorised Professional Practice Police information and records management Code of Practice | College of Policing NPCC Retention and Disposal of Police Records
This Version	V 1.2
Date Created / Modified	30/06/2025
Date Last Approved (SMB)	31/08/2022
Review By	30/06/2028

Contents

Policy

Introduction

Merseyside Police recognises that a high standard of information management is essential to the operational efficiency of the force and is therefore committed to managing its information by having in place organisational structures which will ensure compliance with legislation. The forces records and information are its corporate memory and represent a vital asset to support daily functions, operations and provide proof or evidence of the forces actions and decisions.

National Context

Authorised Professional Practice (APP) is produced by the College of Policing as the official source of professional practice on policing. This policy is to comply with the APP Police Information and Records Management Code of Practice (MOPI). This policy is also supported by the NPCC National Guidance on the minimum standards for the Retention and Disposal of Police Records.

Aims

This policy aims to provide a comprehensive approach to the creation, management, storage and disposal of documents, records and information in all formats across all business areas and functions.

Objectives

- To ensure that all the forces information and records are managed throughout their life cycle in compliance with legislation and national guidance
- To ensure that there is an appropriate information governance structure in place
- To comply with the requirements of the College of Policing Information and Records Management Code of Practice APP and the NPCC Minimum Standards for the Retention and Disposal of Police Records
- To provide guidance on what information should be classed as a record, the timescales to review and appropriate disposal methods
- To ensure all staff are aware of their personal accountability and responsibility for records and information management
- To prevent the unnecessary retention of records and information
- To support the ‘Community First’ philosophy

Application and Scope

All police officers and police staff, including the extended police family and those working voluntarily or under contract to Merseyside Police must be aware of, and are required to comply with, all relevant policy and associated procedures.

This is a non-statutory policy that sets out the principles to help guide decision making. It provides guidance that, on occasions, officers and staff may depart from based on the circumstances they encounter. On such occasions, officers and staff will be supported provided they can demonstrate a clear rationale which can be objectively justified for why they have departed from the policy.

This policy relates to all information and records held in any format by the force. These include:

- Operational policing records
- Corporate records (e.g. HR, legal, financial, ICT data etc)
- Physical records (e.g. paper documents, tapes, CDs, DVDs, photographs etc)
- Electronic records including data held in force IT systems, emails, team drives, website or social media.

Outcome Evaluation

The SIRO (Senior Information Risk Owner) governance board will evaluate outcomes resulting from regular monitoring, taking into consideration:

- Compliance with legislation
- Improvements in the functionality of force systems to manage, review and delete records and data
- Improvements in data quality
- Improved understanding of the benefits of good records management and the risks associated with poor record keeping

Procedure

Version History

Version Number	Date	Detailed rational behind amending/updating policy or procedure.	Policy Owner Details	Policy Author Details
1.0	00/06/22	Initial version. Incorporates Records Management procedures that were originally issued in 2008.	C/Supt Criminal Justice	Records Manager
1.1	00/06/25	New template Introduction added Objectives updated Application and scope streamlined 3.5 Information Assurance Coordinator removed, no longer exists, replaced with Information Security 6.3 remove Information Assurance Coordinator and replace with IAO Section 7 expanded, outline responsibilities of manager & RRD in erasure and rectification 7.1 removal of ACL to records that can't be deleted Section 11 addition of Microsoft Teams channels and One Drives 11.2 incorporated into 11.1 regarding benefits of staff accessing same documents 11.6 addition of who has responsibility to review files in team/Teams channel 11.8 deleted as not required 12.4 reworded 12.6 reworded 12.8 removal of contacting FIM for out of office access, not required 12.10 SOP RAFTS, not required	C/Supt Criminal Justice	Records Manager

		12.11 removed about contacting RMU and not recording on Record Asset and File Tracking database, this is not an option 13.1 addition of reference to RRD policy. Remove 13.2, 13.3, 13.4, 13.5, 13.8 & 13.11 14.2 merged with 14.1, remove 14.3 not required 15.1 list expanded, 15.2 changed from asking RM for advice to assessing archive material 15.3, 15.4 and 15.5 added		
1.2	12/06/26	Updated to reflect new organisational structure; formatting refresh (no change to review date)	C/Supt Criminal Justice	Records Manager

1. Overview

1.1 Good record keeping ensures:

- Records comply with legal and national requirements
- The right information is supplied to the right person, at the right time and in the right format
- Records are adequate, accurate, authentic, secure and accessible; that their evidential weight and integrity are not compromised over time and that they are destroyed when there is no longer a policing or business purpose for retaining them
- The force knows what information and records it is keeping and why

1.2 To achieve this, records need to be managed throughout their life cycle from creation through to disposal.

2. Definitions

2.1 A record is defined as ‘information created, received and maintained as evidence and information by an organisation or person in pursuance of legal obligations or in the transaction of business’.

2.2 The term ‘record’ refers to any information that is created, captured or received that can be used as proof or evidence of business activity, including decisions or in pursuance of legal obligations.

2.3 Records can include (this is not exhaustive):

- Crime and custody records
- Day books and pocket notebooks
- Digital interview recordings, CCTV and BWV footage
- Maps, plans and photographs
- Forms
- Agendas, minutes, decisions, actions and outcomes of meetings
- HR personnel and medical files
- Grievances, disciplinary and capability investigations
- Financial transactions
- Instructions and advice to the force
- Correspondence, reports and advice given/received
- Emails, text messages and social media posts
- Web pages

3. Roles and responsibilities

3.1 The Chief Constable has overall responsibility for the Records Management Policy and procedures and is the forces Data Controller

3.2 The Deputy Chief Constable is the forces Senior Information Risk Owner (SIRO) and is accountable and responsible for managing information risks across the organisation, supported by the Information Asset Owners (IAO). The SIRO will ensure that everyone is aware of their personal responsibility to exercise good judgement and to safeguard and share information appropriately.

3.3 Information Asset Owners must be senior/responsible individuals involved in the running of the relevant business area. Their role is to understand what information is held, what is added and what is removed, how information is removed, who has access and why. As a result, they can understand and address risks to the information, including data quality issues and ensure that information is used fully within the law for the public good and is deleted when no longer required. They provide a written judgement of the security and use of their asset annually to support the audit process.

3.4 The Data Protection Officer is the force expert, providing professional advice and guidance to the organisation on compliance with the Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR); informing and advising the data controller and SIRO of the forces obligations under the DPA.

3.5 The information Security Officers coordinate, develop and implement information assurance initiatives to meet the forces responsibilities for information security to ensure

the confidentiality, integrity and availability of police information and the systems upon which it resides.

3.6 The Records Manager is responsible for:

- Issuing records management policy, advice and guidance and monitoring compliance
- Reviewing and maintaining the force Review, Retention and Disposal (RRD) schedule
- Providing records management advice for new/upgraded IT systems and ensure that record creation, maintenance, review and deletion is both appropriate and practicable
- Managing the forces storage facility for physical records
- Archiving of records deemed suitable for permanent preservation
- Providing direction for the Records Management Team and the RRD team
- Ensuring that any necessary Records Management training needs are identified, and appropriate training provided.

3.7 All supervisory staff are responsible for:

- Ensuring the accuracy of the information that their staff enter into force systems
- Ensuring that records are created, evaluated, maintained, reviewed, retained and disposed in accordance with this policy and any associated Records Management procedures/guidance.

3.8 All staff are responsible for:

- Keeping accurate, complete and secure records stored in appropriate locations, for the appropriate length of time and subject to review.

4. Access to records

4.1 Access to force records and force systems is restricted and role dependent. Criteria for access to individual force systems and compliance monitoring is primarily the responsibility of the Information Asset Owner (IAO) with support from the Data Protection Officer or Information Security Officers as necessary. Access is based on the principle of least privilege, in line with an individual's role. Access should be reviewed on a regular basis to ensure that when staff leave of change roles their access is removed. Access to all force systems is automatically removed when a person leaves the force.

4.2 Access to individual files or boxes of physical records held in store at Edge Lane is restricted to staff in the same department as the recorded 'owning' department i.e. the department to whom the records belong to. For example, Personnel files will on be issued to staff in the People Services Department. If a request is made for a file that does not

belong to the requestors department, the Records Management team will seek permission form the owning department prior to issuing it on loan.

4.3 Access to search or view certain types of record on the Record Asset and File Tracing Systems is restricted to staff in relevant departments.

5. Information Asset Register

5.1 The force maintains an information Asset Register which provides an inventory of all force and departmental systems and documents the data/records maintained on each system as well as providing details regarding access and control of the data.

5.2 The Information Asset Register is a restricted document. If you require access to it, then please contact information.security@merseyside.police.uk

6. Data quality

6.1 To ensure that the principes of the Data Protection Act 20018 are followed, personal data must be:

- Adequate, relevant and not excessive in relation to the purpose for which it was obtained
- Accurate and up to date
- Retained for no longer than necessary

6.2 The force recognises that data quality is integral to effective policing, helps inform better decision making and increases both public and officer safety and confidence. Utilising correct, up to date information can help to avoid civil claims, fines and reputational risk. It improves efficiency around searching/retrieving data and can help avoid missed opportunities, as well as serving legal obligations.

6.3 IAO's will maintain a programme of regular data quality checks that include all systems that process personal data and manual records except for Niche and Corvus which are separately monitored.

6.4 Reports designed to pick up data quality errors are run on Niche and Corvus on regular basis to monitor personal data and ensure that any duplicate nominals or nominals with missing data are identified and corrected.

6.5 The results of data quality reviews will be acted upon to refresh and improve information retention practices and accuracy. This will ensure compliance with UK GDPR and DPA 2018.

7. Requests for deletion of correction of personal data

7.1 The Records Manager is responsible for initiating a review when a request for deletion or rectification by an individual is received. The Records Manager or RRD team will then conduct a review to determine whether the data is legally held and whether it will continue to be retained or deleted. The result will be documented on the National Review Assessment Criteria (NRAC) form that will be linked to the nominal on Niche. If the decision is to delete the data, the West Coast Collaboration (WCC) is notified to ensure that the data is removed permanently from Niche. In circumstances where deletion is not possible links to the nominal and related occurrences will be broken. The Records Manager or RRD team will inform the requestor detailing the reasons for erasure or continued retention and advise them to contact the Information Commissioners Office (ICO) if they are not satisfied with the outcome.

7.2 The Records Manager or RRD team must investigate any potentially incorrect data. They will determine whether the data is incorrect and identify the source of the error. If incorrect data is held on Niche, then it will be rectified by the WCC Niche Data Quality Team by means of a supplementary statement explaining the error and providing the accurate information. If this is not possible e.g. because the error is part of an OEL entry, then the Records Manager will notify the relevant officer/department for them to add a new OEL entry to notify users. A response will be sent to the requestor, either to explain that the data is not erroneous and advise on action that the requestor can take e.g. submit their own version of events. If the data is erroneous, the force will confirm the error and explain the corrective actions taken and the data will be removed from use. Steps will also be taken to implement preventative measures to avoid future errors. The action taken by the RRD team will take place in the knowledge and under the supervision of the Records Manager who will maintain a single record of all requests for rectification.

7.3 All requests from members of the public for erasure or rectification of personal data must be responded to within one calendar month of receipt.

7.4 The Records Manager or RRD team must verify that any request for deletion of a custody image meets the Home Office guidance criteria before deleting the image.

8. Audit

8.1 The force will audit, or quality check its information and records management practices for compliance.

8.2 Due to the volume of systems and data assets, it is not feasible to audit all information, data quality, and records management compliance within a single year. Instead, a risk-based sampling approach will be adopted. This approach will be guided by factors such as force priorities, system status, data protection risk assessments and relevant Home Office initiatives.

8.3 The internal audit team is responsible for undertaking audits and will liaise with the IAO, ICT and the Records Manager as appropriate.

8.4 Additional compliance and monitoring activity are conducted across other business functions to support overall data governance. Areas include information security, physical audits, department supervisor checks, review/update and the correction of data, plus any associated audits carried out by the Internal Audit Team. The outcomes of these activities are reported to the SIRO governance board.

9. Training

9.1 All employees, both permanent and temporary will be made aware of their responsibilities regarding record-keeping and records management. This will be achieved through this policy, guidance on iForce and any associated training where required.

9.2 Training in managing records will be delivered by the Records Manager or Records Team Leader upon request.

10. File naming conventions and version control

10.1 See 'Procedure for File Naming Conventions and Version Control' on iForce.

11. Structuring team drives

11.1 Team drive and Microsoft Teams channels exist to enable multiple staff within a department to access and manage shared documentation efficiently. This supports collaborative working and promotes consistent records management practices across teams. The benefits of this are:

- Individual team members can access and work on the same document
- Reduction in creation and retention of multiple copies and versions of documents stored in personal OneDrive's or individual workspaces which will lead to a significant reduction in storage demand
- Less risk of staff not knowing which is the latest version of a document

11.2 To maximise the usefulness of the team drive and Microsoft Teams channels for storing and retrieving information:

- The structure needs to reflect the activities of the department. Think about what the department actually does and base the hierarchy of the folders on these activities
- Access to a file should not be more than 3 clicks of the mouse. In effect this means having more folders than you would have in a paper filing system but fewer levels to

drill down though i.e. a much broader and flatter hierarchy of folders and files with a maximum of 2 levels of folders, for example:

Level one folder	Level two folder	Level three folder
Admin	Travel	Mileage calculations
		Car registration details
	Catering	Menus
		Refreshments
		Ordering forms
Records Management	Historic Archive	Research replies
		Donations

11.3 Folder and file titles need to be meaningful to all users. Multiple staff need to be able to find the same documentation quickly and accurately.

11.4 Don't have a folder with a single document in it. Delete the folder and make the document directly available at the folder level.

11.5 Don't have folders labelled 'miscellaneous' or 'general'. These will become dumping grounds for files and documents that are unrelated or become the repository for files and documents that should be filed elsewhere in the team drive or Teams channel.

11.6 The administrators of the team drive or Teams channel and/or heads of departments should review the contents on a regular basis (every 6-12 months) and:

- Delete any files or folders that are no longer required
- Check that no-one has created a new folder that duplicates the content of an existing folder and hence started a new filing system within the existing one
- Check that all folders have meaningful titles and are located in the correct part of the folder hierarchy

12. Physical storage

12.1 The force has its own warehouse for the storage of physical records and files at Edge Lane, Liverpool. All boxes that were previously stored with an offsite storage contractor have been returned to the force.

12.2 Edge Lane has been purpose built to accommodate records and evidence and officer and staff should ensure that all documentation that is no longer being worked upon is indexed onto the Record Asset and File Tracking system and set to Edge Lane. The Records Management Unit (RMU) will then take responsibility for its storage, management and ultimate disposal when no longer required.

12.3 Physical records should be stored in appropriate environmental conditions. Records that are stored in unsuitable conditions, e.g. damp or dusty are more likely to degrade more quickly over time and be rendered unusable. All records should be stored securely to minimise the risks of loss, theft or inadvertent destruction and maintain confidentiality and integrity.

12.4 The contents of all boxes stored in Edge Lane are recorded on the Record Asset and File Tracking system. Access to this database is given after the staff or officer has received training in the use of the system from the RMU. If a department or strand want to access the warehouse, they must ask RMU for permission. The RMU team leaders will quality assure records prior to being stored in the warehouse. This ensures that the records are indexed in a consistent manner and are searchable and retrievable in the future.

12.5 The RMU will ensure that the staff resource required to index records is proportionate with the importance of the records and the likelihood that the records will be required in the future.

12.6 To ensure effective management of the warehouse, all departments and BCU's are required to use the Record Asset and File Tracking system rather than maintaining a separate record of items set to Edge Lane. This is deliberate as the warehouse contains 37,000 shelves and requires precise tracking of each boxes exact location. In addition, the use of a single database also brings the below advantages:

- It can link related files across different departments, e.g. connecting an Investigation with corresponding documentation from Scientific Support
- Every file and box are assigned a review/destruction date ensuring uniform retention periods across the organisation
- It minimises the risk of records becoming irretrievable due to forgotten acronyms or operation names
- Provides management and statistical data to ensure the space is used and managed appropriately
- Enables the force to answer external enquiries that may otherwise be unresolvable
- Staff can locate and access records from other departments when required, streamline procedures and reduce time spent on administrative tasks.

12.7 All requests for the retrieval of files and boxes must be made in writing to the RMU. This is to ensure that there is a proven audit trail for each request. The team will locate and dispatch the file/box via the internal mailing system, or the requestor can make

arrangements to collect from Edge Lane. Requests received before 3pm Monday – Friday will be processed the same day where feasible. The internal mailing system however may take up to 2 working days to deliver to the recipient. Requests received after 3pm or at the weekend will be processed the next working day. If a request is urgent, please inform the RMU via telephone.

12.8 Access to the warehouse at Edge Lane is restricted to RMU and Evidence Management Unit (EMU) staff only. Officers and staff who request to collect a file/box must report to the visitor reception at the EMU, Edge Lane. The opening hours are 8am – 4pm, Monday – Friday. There is no access at the weekends or Public Holidays.

12.9 The RMU are responsible for recalling files/boxes that are overdue for return and re-filing records that have been returned. If in the event the information is misplaced or cannot be located at any point the RMU will notify the Information Security Officers who will record this as an Information Security breach.

12.10 Unless informed otherwise, all records stored at Edge Lane are deemed to be classified as 'Official' or 'Official Sensitive' and are stored accordingly; the warehouse has restricted access and is alarmed outside of working hours.

12.11 Edge Lane has the facility to store more sensitive and confidential records within a separate lockable area.

12.12 Advice or assistance is available by contacting the Records Manager, Records Management Team Leaders or the Records Management Team.

13. Review, Retention and Disposal (RRD)

13.1 All force records are required to be retained for the minimum period necessary for legal, operational, research, practical and safety reasons. The length of time will be dependent on the type of records, its purpose and reason for retention. Once there is no longer a policing purpose for continued retention, the records should be destroyed. This will ensure compliance with GDPR and DPA with regards to personal data. Further details are outlined in the Review, Retention & Disposal; Records Management Policy & Procedure.

13.2 The RRD team within the RMU are responsible for the review of crime files and nominals on Niche and any associated paper records. They undertake a programme of scheduled reviews at the end of their retention period to determine if continued retention is warranted or if they should be disposed. Their assessments will be based on the National Risk Assessment Criteria (NRAC) and the rationale for any continued retention will be recorded. Records that continue to be retained will have a new retention period specified and an indication of whether the records will need further reviewing or can then be destroyed.

13.3 The RRD team undertake triggered reviews as necessary. Reviews can be triggered by a number of events such as a request for disposal by a member of the public, a personal data breach, the merging of duplicate nominal records or other observed irregularities. A review will confirm whether there is still a policing purpose for continued retention and arrange for disposal if appropriate.

13.4 RMU staff will take responsibility for the review and disposal of all physical files stored at Edge Lane unless the owning department wishes to undertake the task owing to its sensitivity and confidentiality.

13.5 Some records can be kept beyond the retention period set out in the NPCC retention schedule and transferred to the force archive. See section 15.

14. Physical destruction of records

14.1 There are records that have been earmarked to be preserved long-term, such as policies and policing procedures and they will go into the force archive. All other records will be destroyed at the end of their life cycle. Physical records that are awaiting destruction should be stored securely, locked away to avoid unauthorised access. The basic requirements are list below:

Format	**Protective marking**	**Destruction**
Paper	Official	Place in confidential waste sacks/bin to be collected by the forces approved confidential waste contractor
	Official-sensitive	Torn/shredded and then placed into confidential waste sacks/bin to be collected by forces approved confidential waste contractor
Magnetic media e.g. audio tapes, CD's, DVD's	Official	Place in confidential waste sacks/bin to be collected by the forces approved confidential waste contractor
	Official-sensitive	Destroyed completely and securely
Computer hard drives	Official or official-sensitive	Destroyed completely and securely

15. Archiving and preservation of records

15.1 Records may be held beyond their operationally required retention period for scientific, archiving or historical purposes on a case-by case basis. These records will no longer be used to conduct routine Merseyside Police business. Criteria for archiving include:

- Crime files and evidence relating to a case of local or national importance
- Records that demonstrate major changes to the force
- Significant force policies and procedures
- Records that provide evidence of major projects, functions or activities
- Individuals, national and international events of significant interest or controversy
- Artefacts and memorabilia including:
    - Uniforms, badges, medals and insignia
    - Historical police equipment (e.g. radios, batons, handcuffs)
    - Photographs, negatives and slides
    - Posters, banners and signage
    - Awards, certificates and commendations
    - Personal items donated by former officers or staff
    - Oral histories, diaries and personal testimonies
    - Event materials (e.g. programmes, invitations, commemorative items)
    - Items from community engagement or ceremonial events

15.2 Items to be considered for the force archive must be assessed for their:

- Historical significance
- Public interest
- Legal or evidential value
- Cultural or aesthetic value

15.3 All items entered into the force archive must be indexed and catalogued on the Record Asset and File Tracking system to ensure the force can maintain a comprehensive list and be able to retrieve from the archive if requested. Details to be recorded are the title/description, date range, format and the condition of the item, location and access restrictions. Efforts should be made to avoid duplication in order to maintain the long-term capacity of the storage facility.

15.4 All items in the force archive where feasible will be stored in Edge Lane which is restricted access and managed by the Records Management team. If records or memorabilia are gifted or loaned to an external archive or museum a deposit agreement must be in place which details access and recall procedures along with preservation protocols.

15.5 Decisions concerning artefacts and memorabilia are overseen by the RMU and the Archives & Heritage Board, which is chaired by the ACC.