Records Management (Policy & Procedure)

Publication Scheme Y/N	Government Security Classification (GSCS): OFFICIAL Can be published on Force Website
Department of Origin	Criminal Justice
Policy Holder	Chief Supt, Head of Criminal Justice
Author	Records Manager
Related Information	• Data Protection Act 2018 • Freedom of Information Act 2000 • Criminal Procedure and Investigations Act 1996 (CPIA) • Statute of Limitation Act 1980 • Human Rights Act 1998 • Protection of Freedoms Act 2012 • Regulation of Investigatory Powers Act 2000 • 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 • Government Security Classification Scheme Policy • ICT Acceptable Use Policy • Information Management Strategy • Information Risk Management Policy • Information Security Policy • Records Retention and Disposal Schedule • Home Office Code of Practice for the Management of Police Information (MoPI) • College of Policing Information Management Authorised Professional Practice • The NPCC Minimum Standards for the Retention and Disposal of Records
Date First Approved at SMB	31/08/2022
This Version	V1.0 June 2022
Date of Next Review	June 2025

June 2022

Contents

Policy

National Context

The College of Policing Authorised Professional Practice: Information Management provides generic guidance on the management of all police information including Data Protection, Information Assurance and Freedom of Information. Police information is defined as all information obtained, recorded or processed for a policing purpose.

Statement

Merseyside Police is committed to ensuring good information and records management. It recognises that information is the lifeblood of policing and that the effective management of police information to a high standard is core to efficient policing. The force's records and information are its corporate memory and represent a vital asset to support daily functions, operations and provide proof or evidence of the force's actions and decisions.

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

a) To ensure that all the force's information and records are managed throughout their life cycle in compliance with legislation and national guidance
b) To ensure that there is an appropriate Information Governance structure in place
c) To comply with the requirements of the College of Policing Information Management: Authorised Professional Practice
d) To provide guidance on what information should be classed as a 'record'
e) To reduce costs of records storage and management, including retrieval and controlled disposal

Application and Scope

f) 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.
g) For all police officers, police staff including the extended police family and those working voluntarily or under contract to Merseyside Police who process personal data, it is mandatory that they must read the following policies and procedures upon induction and refresh re-reading them annually.

- Data Protection Policy
- ICT Acceptable Use Policy
- Information Security Policy
- Records Management Policy

Information Assurance Team staff will monitor compliance with this requirement.

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

- All operational policing records

- All corporate records (e.g., HR related, legal, financial, administrative, ICT data)
- All physical records (paper, interview tapes, CDs, DVDs, photographs, drawings etc)
- All electronic records including data held in force IT systems, emails, team drives, website, or on social media

Outcome Evaluation

The SIRO (Senior Information Risk Owner) Governance Board will evaluate outcomes resulting from regular monitoring, taking into consideration the following:

a. Compliance with legislation and national information and records management standards
b. Improvements in the functionality of force systems to manage, review and delete records and data
c. Improvements in data quality and consistency
d. Improved understanding of the benefits of good records management and the risks associated with poor record-keeping

Procedure

Version No.	Date	Detailed rationale	Policy Owner Details	Policy Author Details
V1.0	June 2022	Initial version. Incorporates Records Management procedures that were originally issued in 2008.	C/Supt. Claire Doyle	Kate McNichol

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 is 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" (British Standard ISO 15489: 2016 (2nd edition))

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. Although this is not an exhaustive list, records include:

- Crime, case and custody records
- Day books and pocket notebooks (PNBs)
- 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 (e.g., Area and Departmental Orders, InTouch, People and Policy Matters)

- Correspondence, reports and advice given and received
- Emails, text messages and tweets
- Web pages (intranet and force website)

3. Roles and Responsibilities

3.1. The Chief Constable has overall responsibility for the Records Management Policy and procedures and is also the force's Data Controller.

3.2. The Deputy Chief Constable is the force's Senior Information Risk Owner (SIRO) and is accountable and responsible for managing information risks across the organisation, supported by the Information Asset Owners (IAOs). 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 (IAOs) 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 moved, 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 force's obligations under the DPA.

3.5. The Information Assurance Coordinator coordinates, develops and implements information assurance initiatives to meet the force's responsibilities for information security to ensure the confidentiality, integrity and availability of police information and the systems upon which it resides.

3.6. The force Records Manager is responsible for

- Issuing records management policy, advice and guidance and monitoring compliance
- Reviewing and maintaining the force Retention and Disposal 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 force's storage facility for physical records
- Archiving of records deemed suitable for permanent preservation
- Providing direction for the Records Management team and the Review Retention and Disposal 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 of 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 Assurance Coordinator 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 or 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 the store at Edge Lane is restricted to staff in the same dept as the recorded 'owning' dept i.e., the dept to whom the records belong. For example, Personnel files will only be issued to staff in the People Services Dept. If a request is made for a file or box that does not 'belong' to the requestor's dept, RMU staff will seek permission from the owning dept before issuing it on loan.

4.3. Access to search or view certain types of record on RAFTS (Record Asset and File Tracking System) is restricted to staff in the relevant depts. These include Personnel files; PSD files; Intelligence and Covert Operations.

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 currently a restricted document within iForce. If you feel you require access to it, then please approach information.security@merseyside.police.uk

6. Data Quality

6.1. To ensure that the principles of the Data Protection Act 2018 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 is 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. Information Compliance Officers will maintain a programme of regular data quality checks using the Assurance Map in liaison with Information Asset Owners or their nominee 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 RMS and Corvus on a 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 Article 5(1)(c) UK GDPR and s.37 DPA18.

7. Requests for Deletion or Correction of Personal Data

7.1. See separate document 'Procedure for the Erasure or Rectification of Personal Data'

8. Audit and Dip Sampling

8.1. The force will audit /dip sample its information and records management practices for compliance.

8.2. Due to the volume of systems and data assets, it is not possible to audit all information, data quality and RM compliance in any given year. Instead, a risk-based approach will be taken, dependent on factors such as force priorities, status of a system (e.g., if it's due to be replaced or have a major upgrade), data protection risk assessment or Home Office initiatives.

8.3. The Internal Audit team is responsible for undertaking audits and will liaise with the Information Asset Owner (IAO), ICT, and the Records Manager as appropriate.

8.4. Additional compliance and monitoring activity is carried out within other business functions that supports records management review. 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. Results will be report to SIRO's Information Governance Board.

9. Training

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

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

10. File Naming Conventions and Version Control

10.1. See Separate document ‘Procedure for File Naming Conventions and Version Control’

11. Structuring Team Drives

11.1. Team drives exist to enable multiple staff within a department to have access to the same documentation

11.2. The benefits of this are:

- Individual team members can access and work on the same document
- Reduction in multiple copies and versions of documents being held on home drives or individual workspace in the team drive with consequent reductions in demand for storage space
- Less risk of staff not knowing which is the latest version of a document

11.3. To maximise the usefulness of the team drive for storing and retrieving information:

- The structure of the team drive needs to reflect the activities of the department. Think about what the department actually does and base the hierarchy of the team drive 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 through i.e., a much broader and flatter hierarchy of folders and files with a maximum of 2 levels of folders e.g.

Level One Folder	**Level Two Folder**	**Level Three Folder**
Admin	Travel	MileageCalculations
		CarRegistrationDetails
	Catering	Menus
		Refreshments
		OrderingForm
Records Management	Historic Archive	ResearchReplies
		Donations

11.4. Folder and file titles need to be meaningful to all users. Acronyms may mean something to some people but nothing to others. Multiple staff need to be able to find the same documentation quickly and accurately

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

11.6. Don’t have folders labelled ‘Miscellaneous’ or ‘General’. These will become dumping grounds for all sorts of files and documents that are unrelated or worse become the repository for files or documents that should be filed elsewhere in the team drive

11.7. Review the content of the team drive on a regular basis (suggested timescale is 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 team drive folder hierarchy

11.8. If you require further advice or assistance, please contact the Records Manager.

12. Physical Storage

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

12.2. Edge Lane has been purpose-built for the storage of records and evidence and officers and staff should ensure that all documentation that is no longer being worked upon is indexed onto RAFTS (Record Asset and File Tracking System). and sent to Edge Lane. The Records Management Unit 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 basement or dusty storeroom, are more likely to degrade more quickly over time and be rendered unusable. All records should be stored securely under lock and key, if necessary, to minimise the risks of loss, theft or inadvertent destruction and maintain confidentiality and integrity.

12.4. The contents of all boxes stored at Edge Lane are recorded on RAFTS. Access to the database is only given after the staff concerned have received training in the use of the system from the Records Management Unit (RMU) staff. If a Department or Strand wishes to use the facility, they must ask the RMU for access. The RMU staff will assess their records, consult and advise them on how they should be indexed, and produce a template for indexing. This ensures that the records are indexed in a consistent manner and that they will be searchable and retrievable in the future.

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

12.6. Requiring all Department and Strands to use RAFTS and not allowing them to maintain their own records of what has been sent to Edge Lane is deliberate. The RMU need to be able to manage the storage facility and with over 37,000 shelves they need to know the exact shelf location of every box and RAFTS does this. In addition, the use of a single database has several benefits that would not be realised if departments maintained their own records:

- It can link together related records from different departments e.g., an MCU investigation with the corresponding file from Scientific Support.
- It ensures that all related records are retained for the same length of time – every file and every box has a review / destruction date allocated to it.
- It contributes to the force's corporate memory. By ensuring that there is more than one 'hook' available to retrieve a record, it minimises the risks that the records will become

irretrievable in the future and also ensures that the force is not reliant upon an acronym or an operation name that may become meaningless in a few years' time.

- It provides management and statistical data on the take-up and use of the facility and helps to ensure that the space is managed appropriately.
- It provides a tool that enables the force to answer external enquiries that may otherwise prove impossible to solve.
- It allows staff to search for records that they may need in the course of their work, but which do not originate from their Department or Strand. Thus, RAFTS can streamline procedures and reduce the time needed for a specific task.

12.7. All requests for the retrieval of files or boxes must be made via the RMU. All requests must be made in writing either by submitting a request via RAFTS or by email. This is to ensure that there is a proven audit trail for every request. The RMU staff will locate and despatch the file/box via the internal post, or the requestor can make arrangements to collect it from Edge Lane. Requests made before 3.00pm, Mon – Fri will be processed the same day and the files or boxes put in the internal post. Please note that the internal post may take up to 2 working days to reach you as all post collected from Edge Lane is first taken to Rose Hill and then sent out from there to the relevant stations. Requests made after 3.00pm or at the weekend will be processed on the next working day. If a request is urgent, please phone the RMU to discuss how best to get the information to you.

12.8. There is no access to the store for non-RMU or Evidence Management Unit (EMU) staff. Officers and staff who want to collect a file or box must report to the Visitor Reception at Edge Lane. They will then either be escorted to the store or the file/box brought to them. The opening hours are 9.00 – 16.00, Mon- Fri. There is no access at weekends or on Bank Holidays. If a file or box is required outside of these hours, please contact the Force Incident Manager who will make arrangements for a member of the RMU staff to attend the site and meet you there.

12.9. The RMU staff are responsible for recalling files that are overdue for return and for re-filing all files or records that have been returned.

12.10. Detailed guidance on the operation and management of RAFTS is contained in RAFTS Standard Operating Procedure.

12.11. Unless RMU are informed to the contrary, the records stored at Edge Lane are deemed to be classified as 'Official' or 'Official Sensitive' and are stored accordingly i.e. in a facility where access is restricted to EMU and RMU staff and that is locked and alarmed outside of normal working hours.

12.12. However, Edge Lane does have the facility to store more sensitive records in separate lockable racking within the store. If you require access to this facility, please contact the Records Manager to discuss. Please note, that if you don't want the RMU staff to access these records, an exception to recording the contents of the box(es) on RAFTS can be made, although we will still require the boxes to be registered so that their shelf location is known.

12.13. Please contact the Records Manager or Records Supervisors or email 'Records Management' if you require further advice.

13. Review Retention and Disposal of Records

13.1. All force records are required to be retained for the minimum period necessary for legal, operation, research, practical and safety reasons. The length of time will be dependent on the type of record, its purpose and reason for retention. Once there is no longer a policing

purpose for continued retention, the records should be destroyed. This is particularly the case for the retention of personal data to ensure compliance with UK GDPR and DPA18.

13.2. The force has a Records Retention and Disposal (RRD) Schedule (available on the Intranet) that specifies the length of time that each type of record should be retained. The RRD Schedule takes into account the NPCC National Guidance on the Minimum Standards for the Retention and Disposal of Police Records as well as operational and legal requirements and has been drawn up in consultation with staff in Departments and Strands.

13.3. The RRD Schedule is subject to periodic review, but amendments and additions can be made at any time. If there is no entry on the RRD Schedule for a specific type of record, staff should seek advice from the Records Manager.

13.4. Information Compliance Officers will maintain a programme of data mapping to ensure that the RRD Schedule and the RRD entries within the Record of Processing Activity mirror each other. If they discover that there is processing of personal data that is not covered by the RRD Schedule, they will notify the Records Manager. The Records Manager will assign a retention period, inform the Information Compliance Officers accordingly and update the RRD Schedule.

13.5. The RRD Schedule indicates if the records can be destroyed at the end of the retention period or whether they should be reviewed first.

13.6. There is a separate Review Retention and Disposal (RRD) team within RMU who are responsible for the review and deletion of all crime files on Niche and any associated paper files. They will undertake a programme of scheduled reviews to review files 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.

13.7. The RRD team will also 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.

13.8. The work of the RRD team will be independently audited by staff in the RRD teams from the other forces linked to the Niche West Coast Collaboration who will dip sample the completed reviews.

13.9. RMU staff will take responsibility for the review and disposal of all other physical files stored at Edge Lane unless the owning dept wishes to undertake the work.

13.10. Some records should be kept permanently and transferred to the Force Archive. See the section on ‘Archiving and Permanent Preservation’ above.

13.11. Please contact the Records Manager if you need further advice or information on any aspect concerning the retention, review, or destruction of records.

14. Physical Destruction of Records

14.1. There are a few records that have been earmarked to be preserved permanently (such as policies and policing procedures) and these will eventually go into the Force Archive. All other

records will be destroyed at the end of their life cycle. There is more detailed guidance available in the Force's Information Security Policy and Procedure but the basic requirements for destruction are given in the table below.

Format	**Protective Marking**	**Destruction**
Paper	Official	Place in confidential waste sacks to be collected by the force's approved confidential waste contractor
	Official-sensitive	Torn or shredded and then put into confidential waste sacks to be collected by the force's approved confidential waste contractor
Magnetic media – e.g., audio tapes, videos – and CDs or DVDs	Official	Place in confidential waste sacks to be collected by the force's approved confidential waste contractor
Magnetic media	Official-sensitive	Should be destroyed completely and securely. Obtain advice from the Information Assurance Coordinator
Computer hard drives	Official or Official Sensitive	Should be destroyed completely and securely. Obtain advice from the Information Assurance Coordinator

14.2. Physical records that are awaiting destruction should be stored securely in a locked room to avoid unauthorised access.

14.3. Please contact the Records Manager or Records Supervisor or email 'Records Management' if you require further advice.

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. However, 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

15.2. If you have any documentation or artefacts that you think should be preserved in the force Archive, contact the Records Manager to discuss.