WILTSHIRE POLICE & POLICE AND CRIME COMISSIONER

RECORDS MANAGEMENT POLICY

Date of Publication: May 2022
Version: 6.0
Next Review Date: May 2024

TABLE OF CONTENTS

POLICY STATEMENT

Wiltshire Police and the Office of the Police and Crime Commissioner (OPCC) recognise that the efficient management of records is necessary to comply with legal and statutory obligations, the Management of Police Information (MoPI) Code of Practice, Authorised Professional Practice (APP) Information Management, Guidance and other Codes of Practice. Dynamic records management contribute positively to the performance, efficiency and effectiveness of the overall business management through:

a) Supporting policy formation and decision-making
b) Protecting the interests of the force and the rights of individuals (staff and members of the public)
c) Facilitating consistent and equitable delivery of service

Records Management Within Wiltshire Police and the OPCC

Information, knowledge and intelligence are the lifeblood of policing. Once captured, they must be systematically managed as business records according to the policy and standard working principles highlighted within this document.

The integrity of police information relies on the information being trusted, acceptable, useable and available. It should be in a format that is accessible and easy to use, whether it is an electronic, photographic or paper format.

The purpose of records management from policing and business perspectives is to ensure that information is documented and maintained in such a way that its evidential weight and integrity is not compromised over time. To achieve this, records must be managed throughout their lifecycle, from creation through to disposal.

Applicability

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.” (BS ISO 15489-1: 2001 – British Standards around Information, Documentation and Records Management).

Although not an exhaustive list, examples of items that can constitute records include: -

- documents (including written and typed documents and annotated copies)
- computer files (including word processor files, databases, spreadsheets and presentations)
- electronic mail messages
- notebook records (including One Note and ‘blue books’)
- fax messages
- brochures and reports
- intranet and Internet Web pages
- forms
- seized evidence
- audio and video tapes, including CCTV
- microfiche and microfilm
- maps and plans
- photographs

This policy, together with the associated standards, applies to the management of all operational and business records (whether containing personal data or not) in all technical or physical formats or media, collected, received, created, held, shared, disseminated, disclosed, maintained, reviewed,

retained or disposed of by staff of Wiltshire Police, the OPCC and 3rd parties in the course of carrying out the functions of the organisation. All police officers, police staff, OPCC staff, service provider staff and those working voluntarily or under contract to Wiltshire Police must be aware of, and are required to comply with, this policy.

This policy does not apply to copies of documents published by other organisations that are kept for reference purposes only.

Risk Assessments / Health and Safety Considerations

There are no risks associated with the implementation of good records management procedures.

The risks associated with not following good records management procedures are:

a) inability to ensure that records are present, accessible, capable of being interpreted, trusted and maintained through time
b) health and Safety / Environmental risks associated with the storage of large amounts paper incorrectly and / or unnecessarily (e.g. trip hazards, blocking exits and risk of fire)
c) criminal Justice outcomes being prejudiced
d) inability to comply with legislative and Regulatory body expectations (e.g. MoPI, Data Protection, Freedom of Information, VAT rules etc.)

This policy aims to minimise the above risks as much as possible.

Record Characteristics

Records owned and managed by Wiltshire Police and the OPCC provide organisational memory, evidence of actions and decisions and represent a vital asset to support daily functions and operations. Wiltshire Police and OPCC records will be compliant with BS ISO 15489-1:2001 and will be complete, authentic, reliable, secure, usable, have integrity and be accessible. These records will be managed in accordance with good practice and legislative requirements ensuring they remain credible and authoritative throughout their lifecycle.

It must be possible to prove that records are what they purport to be, to demonstrate that their integrity is intact and to identify the originator. Where a record is amended, an audit trail will be created.

Records will accurately reflect the transactions that they represent.

The Force and OPCC will seek to comply with other national and international standards such as BS 10008:2014 – Evidential Weight and legal admissibility of electronic information and BIP 0025:2002 – Effective Records Management (this list is not exhaustive).

Records will be securely maintained to prevent unauthorised access, alteration, damage or removal. They will be held securely according to their Classification in accordance with the requirements of the Government Security Classification Scheme (previously Government Protective Marking Scheme).

Records will be reviewed and disposed of promptly in accordance with the Records Retention Schedule and an audit trail kept.

Records management systems will provide an auditable trail of records transactions from creation through to ultimate disposal.

Records will be readily available and sufficient in content, context and structure to provide sufficient, authenticated evidence of the relevant activities and transactions. This includes the preservation of physical records, the migration of electronic records and the accurate cross referencing of hybrid records (part paper, part electronic).

The term “readily available” is **not** the same as immediately available. The speed at which records can be retrieved will depend on where, how and in what format they are stored. Files or tapes may have to be retrieved from offsite Archive Facilities, both of which may take several days.

Systems that are routinely used for records management will support these characteristics and be comprehensive, systematic and compliant with all requirements arising from current business. The Force and OPCC will make the best use of available technologies to assist in the efficient management of records.

The intelligent application of records management standards and principles will lead to the retention of few records. However, those records will be of a higher quality, be more useful as evidence and be a reliable source of information on which to base decisions.

Records for Law Enforcement Purposes

For the purposes of the Data Protection Act 2018 Part 3 governs information that is required for Law Enforcement Purposes.

Law Enforcement Purposes are defined as:

- prevention, investigation, detection or prosecution of criminal offences, or
- execution of criminal penalties, including the safeguarding against and
- prevention of threats to public security.

These purposes are not mutually exclusive. Information can be collected for one Law Enforcement Purpose and used for another that may not have been known about at the point of collection. It is essential that in order for information to be legally held, a lawful purpose is established.

Generally, if the processing is necessary for the performance of a task carried out for the following purposes; law enforcement, a legal obligation, the administration of justice, the safeguarding of children and of individuals at risk, a contract or the data subject has given consent then the processing will be lawful (for more information see the Data Protection Policy).

The Management of Police Information (MoPI) guidance applies to records held within the business areas of crime, intelligence, custody, domestic violence, child abuse investigation, firearms revocations and refusals. There will be additional business areas to which the MoPI principles are to be applied. However, information that is ancillary to a Law Enforcement Purpose (i.e. personnel, finance etc.) is not included under MoPI.

Historical data is defined in MoPI as anything recorded prior to April 2006. The back record conversion (BRC) of historical data held for a policing purpose will be prioritised based on risk. Low priority historical data, where the cost of BRC greatly outweighs the potential risk, will remain subject to time-based disposal, where applicable.

Record Creation

Good quality information collected, recorded, evaluated, shared, reviewed, retained and disposed of is essential to support our policing and organisational objectives. It is essential that our information can be shared with and used confidently by other Forces and agencies.

The Force and OPCC will comply with APP by ensuring information entered onto a record (paper or IT based) conforms to the following:

- information is recorded for Law Enforcement Purposes
- information is recorded in the appropriate format for the business area in which it is held
- information is recorded according to the data quality principles – accurate, adequate, relevant and timely
- checks are made to avoid creating duplicate records
- links are made to existing records
- correct GSC marking is used

Compliance with APP on record creation and local Data Quality standards is the responsibility of everyone who enters new data onto police databases. This important principle should be conveyed and reinforced in initial training and in subsequent practice. It will be the line manager's responsibility to carry out regular dip samples to check that their staff record information to the required standard. Where the standard is not being met, feedback should be given, and where necessary, appropriate training or guidance arranged using the Personal Development Review process.

Each operational/business area will have in place clearly worded and effectively disseminated procedures, rules and conventions relating to each police system/process in that area. These procedures will take into account the legislative and regulatory environments in which the operational/business area works and include controls to ensure each record is created using the appropriate templates, forms or database.

Information received from other agencies will be treated and evaluated as a piece of intelligence.

Storage

All records created by Wiltshire Police and OPCC employees or service provider staff for a work purpose remain the property of Wiltshire Police and OPCC. They must be searchable and retrievable in order to comply with legislation (i.e. Data Protection Act, Freedom of Information Act etc.)

Wherever possible, records will be stored electronically and source documents only retained where there are compelling operational or legal reasons for doing so. In circumstances where individual records cannot be separated out, for example police pocket notebooks, the entire collection of records should be retained according to the most serious offence they contain.

Once information becomes a record, it **must** be stored in appropriate, secure, shared (where feasible) areas (i.e. SharePoint), rather than in "My Documents", Outlook folders, Desktops, One Note or desk drawers, and any draft notes deleted As a general rule, Niche RMS / other operational line of business Applications (for example Storm) should be used to process operational information. Sharepoint / other line of business Applications (for example Origin) should be used for non-operational records.

Legacy operational information is accessible through the Force Data Search (FDS).

Metadata

Metadata is supplementary data about a record. It may be descriptive metadata, which aids searching (e.g. subject or date created), or it may be technical metadata, which aids with the management of the record over time (e.g. disposal schedule, access rights or preservation details).

All records will be tagged with appropriate descriptive and technical metadata, including protective marking category and disposal schedule.

Metadata should be based upon a business classification scheme or file plan and should stay with the record until the point of disposal when the record is no longer needed for business purposes.

Information for a Law Enforcement Purpose (as defined by DPA) will be collected, recorded and linked in accordance with the MoPI Guidance during the initial review. Niche RMS will be the primary repository of Law Enforcement Purpose data.

Preservation of Physical Records

The tracking (movement and location of physical records) will be managed by the Operations Manager, Justice Division to ensure that any record can be:

- easily retrieved at any time
- and that there is an auditable trail of record transactions

The long term preservation of physical records depends largely upon the environment in which they are stored. The following factors can all cause the premature degradation of physical records (e.g. paper, photographs & negatives, exhibits and audio/visual media):

- adverse temperatures
- fluctuations in relative humidity
- exposure to light
- pest infestations (insects or vermin)
- mould
- pollution
- the stability, acidity or impurity of the paper
- the quality of the storage wallets, folders and boxes used
- incorrect handling

The Operations Manager (Crime Justice & Standards) will ensure equipment and facilities used for current records storage is fit for purpose and safe from unauthorised access, meeting fire regulations and providing reasonable protection from water, rodent or other damage, at the same time permitting maximum approved accessibility to the information and commensurate with its frequency of use.

A business continuity plan must be in place to provide protection for records which are vital to the continued functioning of the Force.

Exhibits

Exhibits will be stored in accordance with the Force Policy and Procedure for the Seizure, Storage Retention and Disposal of Special Property.

Preservation of Electronic Records

The preservation of electronic records presents a more complex challenge, known as digital obsolescence. Not only must one preserve the physical storage medium (e.g. CD ROM), but one also requires the hardware on which to play the media (e.g. CD drive) and software to read the data on the media and present it to the user in a comprehensible way (e.g. a compatible version MS Word etc.). The absence of any one of these three conditions will make the record irretrievable. Once digital obsolescence has occurred, even if the situation can be remedied, it is often extremely expensive to do so.

One solution to digital obsolescence is to store data on networked servers and migrate data onto new media and software as technology advances. This is particularly effective in organisations where the information contained within records is more important than the way that information is displayed. Where records are migrated across changes in technology, the Force will ensure that they remain authentic and accurate. If this is not possible, the reason and risk to the organisation will be fully documented by the Information Asset Owner.

To minimise the risk of records being overlooked during a migration exercise, electronic files should not be stored on local drives / discs or removable media unless there is a genuine business need (i.e. sealed master discs for use in court cases). Where files are created and/or updated using mobile or portable computing devices (e.g. laptops), it is the responsibility of the user to ensure that these files are transferred onto the central system within 72hrs so that they can be backed up. Users should be aware that until the files are backed up, they remain at risk and could potentially be lost in the event of a problem with the portable device.

It is the responsibility of business area leads to ensure that the information held within their IT systems can be and is preserved over time. The requirement to preserve electronic information in accordance with the Force's disposal schedules **must** be incorporated into the *Statement of Requirements* for all future procurement of electronic data management applications.

All line of Line of Business Applications are backed-up. However this does not mean that the information is in a format that can be swiftly accessed following a disaster. An ICT Service Continuity Plan exists to cover a small number of Applications, ensuring that the core business would be supported in the event of a major incident. It is the responsibility of each department to ensure that their business continuity and disaster recovery plans provide adequate contingencies for the ICT systems that the department owns and/or uses, if they are not covered by the overall Force ICT Service Continuity Plan.

Scanning

The scanning of paper records is a time-consuming process, which will only be undertaken where there is a genuine business need, such as:

- the need to create space by disposing of the original paper record or
- the need to share the record on a regular basis between business areas located in different parts of the county.

Any department considering a scanning project must consult with the Information Asset Owner to ensure the business needs are met, and with ICT to ensure that there is sufficient capacity within the ICT infrastructure to safely store the volume of files, that accessing the files is not detrimental to the performance of the network and that resources exist to back up the files appropriately.

Where scanning results in the disposal of the original record, care must be taken to adhere to the scanning standards set out in BS 10008:2008 (code of practice for legal admissibility and evidential weight of information stored electronically).

Scanned copies must be checked for quality before the original is disposed. The original must be retained if:

- a scanned image of sufficient quality cannot be obtained;
- the scanned image requires significant enhancement;
- the record has physical amendments that have not been captured (e.g. pencil annotations that do not show up properly, or Post-It™ notes);
- fraud is suspected;

- there are legal reasons for retaining the original (e.g. contracts)
- the scan is of an exhibit (e.g. a hate-mail letter)

Originals of scanned, non-Wiltshire Police or OPCC records should, wherever practicable, be returned to the originator rather than destroyed.

Where the original is retained after scanning, the scanned version is nothing more than a "convenience copy" and scanning standards need not be so rigorously applied.

Hardware used to scan records will allow the Force and OPCC to adhere to the standards set in BS10008:2014. Where it is intended to dispose of the original record after scanning, multi-function scanner/printer/copier machines will **not** be used.

Email

The management of email and the associated email archive is covered in the Acceptable Use Force Systems Policy.

Access and Security

The legal and business environment in which the Force and OPCC operate establishes broad principles on access rights, conditions and restrictions. The standard business model of preserving the Confidentiality, Integrity, Availability (CIA) and non-repudiation (of origin, content and receipt) should be followed when handling force information and assets. In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorised individuals. All staff have a responsibility to ensure that records are classified and handled in accordance with this environment and are protected from unauthorised access, disclosure and loss.

Electronic and physical records will be made available for continuity of actions, with originators and managing individuals or groups having need to know and use access to information.

The Government's Security Classification system (GSC) applies to all force records and information and will be complied with at all times. Roles / functions within force identified as being competent and authorised to make assessments should decide on the sensitivity / protective marking of a record. This judgement could be on an entire series of records or on an individual record. In all cases, it will identify limitations / restrictions on the records and will highlight groups or individuals who should have access.

The need to ensure appropriate access controls will be managed by assigning access status (privileges and attributes) to both records and individuals. This will ensure that:

- records are categorised according to their access status at a particular time
- records are only released to those who are authorised to see them
- encrypted records can be read as and when required and authorised
- records processes and transactions are only undertaken by those authorised to perform them and
- parts of the organisation with responsibility for particular business functions specify access permissions to records relating to their area of responsibility.

Any judgements for withholding or masking information must be recorded and the resulting record must be maintained for at least as long as the information in question.

The Force and OPCC will not seek to put blanket restrictions on a record series where only some of the individual records are judged sensitive. However, where there is a requirement to use blanket restrictions for genuine technical reasons, they may be used.

The monitoring and mapping of user permissions and role based functional job responsibilities is a continuing process which occurs in all records systems regardless of format. Information Asset Owners will assign individuals access privileges.

Information abstracted from records or record metadata may be subject to legislation requiring it to be either withheld or made more widely available outside normal business needs, or even outside the Force itself. For example, compliance with Data Protection & Freedom of Information legislation.

All records are part of the corporate memory. Unless restricted/limited due to legislation or as a result of judgement/sensitivity (need to know and use principle), they should be made readily available within force. This may be subject to volume restrictions because of technical limitations or copyright reasons. Any access arrangements will be made for a specified duration and these will be reviewed according to a schedule identified during appraisal.

All personnel must be security cleared / vetted before being allowed access to information. This need for security clearance / vetting will be reflected in the role profile.

It may be necessary to grant third parties access to Force records. There may be a requirement for third parties to be security cleared / vetted prior to accessing certain Force records and some records may require redaction prior to sharing. Third party access to Force information will be managed by the business area which created and owns the records in question.

Information for Law Enforcement Purposes will be shared in accordance with Information Sharing Agreements set up between the Force and its partner agencies under MoPI.

Review, Retention and Disposal

The principles of review, retention and disposal will apply to all Force and OPCC records (operational and business) and will be assigned a retention/disposal schedule.

MoPI guidance on review, retention and disposal relates to information held on all police systems other than PNC. The review, retention and disposal of information on the PNC must be conducted in accordance with the PNC Retention Guidelines.

Specific guidance on the review, retention and disposal of MoPI defined information is available in the Force Procedure for MoPI Review, Retention and Disposal.

The **Review** process is the examination of a record to ensure:

- there is a continuing lawful or business purpose to retain
- the record is adequate, accurate, relevant, up to date and not excessive – records that are found to be inaccurate will, where systems allow, be corrected
- all records containing personal data are compliant with data protection principles
- a future date is set to review the record if appropriate

The **Retention** process will incorporate the continued storage of and controlled access to information held following a review. The main principles supporting this process are:

- all records will be held in line with the Force retention/disposal schedule, any decisions to retain for longer than that specified will be fully documented for audit purposes

- due regard will be given to the requirements and implications of relevant legislation (for example the Criminal Procedures Investigation Act 1996)

The **Disposal** process will incorporate the removal of information from all police systems to the extent that the information cannot be restored. As a general principle, records and any copies (physical or electronic) are disposed where it is deemed that they:

- are no longer necessary for a policing/business purpose
- are deemed to be disproportionate/excessive to the purpose they serve
- are inaccurate beyond alteration
- are duplicates

Material that contains personal data will be treated as confidential waste and disposed of in accordance with Force policy.

Please note that there are currently retention protocols in place outlining the types of records that are to be kept outside of usual retention policies if they are (or may be) of interest to:

- **the Public Inquiry into the death of Dawn Sturgess and Salisbury Poisonings (Novichok);**
- **the Public Inquiry into the Response to the Covid 19 Pandemic.**

Records that fall within the scope of these enquiries must not be destroyed. For more information, please refer to the Force Records Manager.

ROLES AND RESPONSIBILITY

Wiltshire Police and the OPCC have a corporate responsibility to own and manage all information created, received and held for business and Law Enforcement Purposes in accordance with the regulatory environment. The Chief Constable is the **Data Controller** for Wiltshire Police records. The Police and Crime Commissioner is the **Data Controller** for the OPCC .

Expectation of All Staff

The Chief Constable has delegated responsibility for records management across Wiltshire Police and the Police and Crime Commissioner for the OPCC. It is the responsibility of **all police and service provider staff** to ensure that:

- all information created, received and held, for which they are responsible is secure, accurate, relevant, kept up to date and retained or disposed of in line with Force policies/procedures and the Retention Schedule;
- they are aware of and implement Force Information Management policies and procedures;
- information is recorded for Law Enforcement Purposes (in accordance with DPA), in the correct format and in a timely and efficient way.

You should:

- understand and abide by your legal obligations under the Data Protection Act 2018 and the Freedom of Information Act 2000
- understand and handle information in line with the Government Security Classification rules
- understand the College of Policing APP on Information Management
- know where to find published guidance and how to use it

- follow good practice in labelling, storing, sharing, protecting and preserving information
- when appropriate, make a written record of information known to make it easier and more reliable to share with others, or to ensure that actions or decisions made at the time can be understood in the future
- understand and follow the Force's Acceptable Use of Force Systems Policy when using any Wiltshire Police ICT equipment
- understand how to use the ICT provided by the Force for your role
- follow the System Operating Procedures for any Wiltshire Police ICT that you use
- report any risks and areas of concern. Everyone in Wiltshire Police and service provider staff has a responsibility to report inappropriate access, use or disclosure of information, in accordance with the Code of Ethics and the Competency and Values Framework (CVF)
- remember the importance of good personal security, information security, operational security and communications security at all times, whether on duty or off and whether using Wiltshire Police ICT or your own equipment

The Senior Information Risk Owner **(SIRO)** is the Deputy Chief Constable. The SIRO is responsible for the setting the information risk appetite and risk tolerance parameters.

Each Business Area Lead nominated as an Information Asset Owner **(IAO)** by the SIRO will ensure that processes exist to control access, so that only those with the appropriate training, knowledge and skills can access and use the information held in their business area. Refer to the Information Risk Management Policy for terms of reference for SIRO/IAO.

The **Records Manager** and the **Operations Manager, Crime, Justice Standards** will jointly provide advice and leadership in the maintenance and development of records management facilities, standards and practices in order to secure the Force's compliance with records management legislation and guidance.

The **Records Manager** will

- provide a single point of contact for all matters relating to Records Management and leadership of the Records Management and the Data Quality/Business Support Teams
- review and maintain operationally the Force Policy on Information Management
- review and maintain the Force Policy for Records Management, Information Review, Retention and Disposal (RRD) and Data Quality Standards
- jointly with all departments maintain the Force Retention schedule and Information Asset Register
- undertake and record detailed audits of randomly selected business areas across the force to ensure that Managers are:
  - conducting regular audits for data quality assurance
  - checking for compliance with relevant Force policies and procedures and
  - reviewing/retaining/disposing of information held in their business area in accordance with the Force retention schedule

The **Operations Manager, Justice Division** has responsibility for the management of all physical records held under that command, to include the Force Archive Facilities, Traffic, Integrated Prosecutions Team and Special Property, although ownership of those records rests with the originating business area. The Operations Manager, Justice Division will;

- provide a single point of contact for Archive and Special Property Records Management;

- review and maintain a Procedural Guidance for the Management and review/disposal of Physical (Special) Property Records and assets
- monitor and review systems in place for special property records management in order to make improvements
- jointly with the Records Manager maintain the Force Retention schedule (as it relates to special property)

All business area leads/departmental managers have ownership of records within their business area. Where there is no clearly defined business owner of a record, the Records Manager will decide appropriate ownership.

All business area leads / managers will:

- ensure that all information and assets created, received and held, for which they are responsible, is secure, accurate, relevant, kept up to date and reviewed/retained or disposed of in line with the Force Records Retention Schedule.
- ensure that all officers and staff are involved in the implementation of records management through internal communication, profile raising, publicity and training
- ensure that appropriate resources are available to properly maintain their business area's records
- publish accurate procedural guidance, support and tools designed to help each person in that business area manage and use the information effectively and in accordance with the APP on information management, relevant policies and supporting SOPs and Guidance. Where local procedures dictate a deviation from the APP on information management, the full rationale will be documented and authorised in the relevant procedural guidance
- conduct and record periodic data quality assurance audits on the information held in their business area to ensure that Data Quality Standards and recording principles are complied with and utilise performance information to provide feedback and support where appropriate
- conduct and record annual audits of the information held in their business area to ensure the ongoing compliance with the Force Records Management Policy, the Force Records Retention Schedule and other appropriate local and national policies and procedures
- ensure that the records in their business area are backed up, that disaster recovery processes are in place and that the records can be preserved over time

The **Data Quality/Business Support Team** undertake non technical support to Niche RMS and detailed research, analysis and updating of Niche to ensure that data recorded is accurate, relevant and up to date including the merging of duplicate data, correction of poor data entries, identifying and rectifying overwritten data and where necessary deletion of inaccurate data.

Records Management Decision Makers conduct nominal focused reviews by critically assessing all crime and incident occurrences, intelligence submissions, command and control and firearms records together with other information and then assimilate it all before making a documented and auditable decision, primarily about the level of risk the individual poses to the community and which MoPI Group (1 to 4) should be assigned. They will also provide support to the Records Manager by responding to records management enquiries, providing advice and guidance and escalating to the Records Manager where appropriate.

Audit Trails

Audit trails will be provided for all records and documents. They should be kept securely and should be available for inspection by authorised personnel.

Audit trails will be managed since they may be of critical importance to the organisation. Claims of compliance may be discredited if the audit trail is not treated correctly and cannot be interpreted unambiguously.

The audit trail will include a record of all relevant occurrences and will be secure. If any significant occurrence is not audited, then the whole audit trail can be discredited and as a direct result all or any information held within the system will also be able to be discredited. For all audit trail data, it will be possible to identify the processes, enabling technology and individuals involved and the time and date of the event.

POLICY AIM

To competently record and manage all information held for policing activity in an efficient and consistent manner to support the objectives and vision of Wiltshire Police and the OPCC and ensure that national and local objectives are met.

LEGAL BASIS AND DRIVING FORCE

Key drivers for this policy and the need for a consistent approach are legislative, particularly the eight principles of the Data Protection Act 2018 and the College of Policing (COP) Authorised Professional Practice (APP) on Information Management. A failure to record, retain, review and dispose information appropriately may constitute a breach and, ultimately, undermine public confidence in the Force.

RELATED POLICIES, PROCEDURES and OTHER DOCUMENTS

This document has been drawn up within the context of:

- Information Management Policy
- Acceptable Use of Force Systems Policy
- Records Retention Schedule
- Information Asset Owners Handbook
- Information Sharing Policy
- Information Risk Management Policy
- Niche RMS Minimum Data Quality Standards
- ISO 15489-1:2001 (Information and documentation - Records management - Part 1)
- ISO 17799:2005 (Information technology - Security techniques - Code of practice for information security management)
- BSI BIP 0025-1:2002 (Effective records management. A management guide to the value of BS ISO 15489-1)
- BSI BIP 0025-2:2002 (Effective records management. Practical implementation of BS ISO 15489-1)
- BSI BIP 0008:2004 (Code of practice for legal admissibility and evidential weight of information stored electronically)
- BSI BIP 0009:2004 (Legal admissibility and evidential weight of information stored electronically. Compliance workbook)
- BSI BIP 0010:2004 (The principles of good practice for information management)
- Force Information Security Policy (FISP),
- NPCC Governance & Information Risk Baseline Standards
- Quality Assurance and Audit (QA),
- Force Systems Operating Protocols (SOPs)

AUTHORISED PROFESSIONAL PRACTICE

Information Management

DATA PROTECTION

Any information relating to an identified or identifiable living individual recorded as a consequence of this policy will be processed in accordance with the Data Protection Act 2018, General Data Protection Regulations and the Force Data Protection Policy.

FREEDOM OF INFORMATION ACT 2000

This has been classed as suitable for public release.

MONITORING AND REVIEW

This Policy will be reviewed and updated by the Records Manager every two years.

WHO TO CONTACT ABOUT THIS POLICY

The Head of Information Management and Assurance and the Records Manager are responsible for this policy.

All queries relating to this policy should be directed to the Records Manager or Force Policy Officer.

DOCUMENT ADMINISTRATION

Ownership:

Department Responsible:	Information Management and Assurance
Policy Owner	Head of Information Management & Assurance
Policy Author:	Records Manger
Technical Author:	Policy Officer
Senior Officer/Manager Sponsor:	SIRO

Revision History:

Revision Date	Version	Summary of Changes
25.05.2022	6.0	Policy extended to reference OPCC Review, Retention and Disposal section text and requirement on the moratorium on the disposal of information relating to on-going Inquiries into Child Sexual Abuse / Undercover Policing removed.
22.08.2022	6.0	Reference and links to the public enquiries into the death of Dawn Sturgess/Salisbury Poisonings (Novichok) and the Response to the Covid 19 Pandemic added to page 11.

Approvals:

This document requires the following approvals:

Name & Title	Date of Approval	Version
Force Policy Officer	25.05.2022	6.0
Head of Information Management & Assurance	04.06.2019	5.0
JNCC (Not required for all policies)	N/A	

Distribution:

This document has been distributed via:

Name & Title	Date of Issue	Version
E-Brief		
Email to relevant affected Staff/Officers		
Other: (state method here)		

Diversity Impact Assessment:

Has a DIA been completed? If no, please indicate the date by which it will be completed. If yes, please send a copy of the DIA with the policy.	☒**Yes** ☐**No** **Date**:

Consultation:

List below who you have consulted with on this policy (incl. committees, groups, etc):

Name & Title	Date Consulted	Version

Implications of the Policy:

Training Requirements

None.

IT Infrastructure

None.