Force Policy

Document title: Records Management

Document Reference: 09/273

Owner: Head of Information Management

Review date: November 2020 v0.9

This Force policy is suitable for public disclosure under the Freedom of Information Act 2000

This document sets out principles to help guide decision making and in some parts may be quite prescriptive. However, it is vital that officers and staff have the freedom to innovate, exercise discretion and take risk based decisions centred on the needs of the victim and the merits of each case.

There may be occasions when a member of staff is considered to have acted outside of the content of this document but if they have done so with honesty, integrity and professionalism, to make the best decision for the community we serve, they will be trusted and supported. On the occasions when this is the case, the rationale for it must be properly recorded.

This document should be read in conjunction with the Force Policy Statement.

Introduction

Information, knowledge and intelligence are the lifeblood of policing. Once captured, they must be systematically managed as business records according to a records management policy that evolves and constantly adapts to emerging technologies, changing best practices and guidance.

Derbyshire Constabulary manages its records to comply with its legal, statutory and other obligations including the College of Policing's Applied Professional Practice APP/MoPI Code of Practice; the Data Protection Act 2018; Freedom of Information Act 2000, Protection of Freedoms Act 2012, and other relevant legislation and industry standards.

Records comprise *organisational memory*, providing evidence of (trans)actions and decisions. They are a vital asset in supporting the force's daily functions and operations. They can be stored in many formats and locations (e.g. digitally in the cloud or on social media sites; on removable media/drives, or physically in a locked cabinet, cupboard or storeroom, or in offsite warehouses managed by a third party; or even any combination of all these, in so-called hybrid (or mixed) environments).

This policy is comprehensive and has been adapted to accommodate emerging new technologies. While it has been written for a wide range of audiences, there is no initial need to read the document in its entirety. Initially, reading the sections **highlighted in bold** immediately below will ensure that you focus on the essentials. You can read the remaining areas as and when required.

What this Policy covers

- Strategic Aim and Objectives
- **Scope of policy**
- **What *are* records?**
- **Why records are important**
- **Police records management in a digital cloud world**
- **Benefits of effective records management**
- **Risks of poor records management**
- **General principles**
- **Roles and responsibilities (Governance)**
- Records Management Programme
- **Best practices**
- **Review, Retention and Disposal (RRD)**
- **Access and Security**
- Learning and Development
- Audit and Compliance
- Appeals Process
- Appendix 1 - Records Management Glossary
- Appendix 2 - Relationship with other relevant existing policies, legislation and standards

Policy Statement

Strategic Aim

Aligned to the force Information Management Strategy (IMS) and accompanying standards, this policy ensures that all information held for policing activity is competently recorded and managed effectively and consistently to support the force's business activities and ensures that national and local objectives are met.

Strategic Objectives

Regardless of the storage media or location, the strategic objectives of this policy are to:

- ensure that all officers and police staff understand that police records and property belong to the force and may not be disposed of without formal prior approval by the relevant manager or executive board as appropriate.
- ensure that within all force business areas information is lawfully held and is readily accessible on demand
- promote effective and consistent management of all records throughout their lifecycle
- ensure all information is captured and maintained in such a way that its evidential weight and integrity is not compromised at any time
- promote auditable decision making
- maintain best practice information management
- reduce costs of records storage and management, including retrieval and controlled disposal
- ensure that records are appropriately protected and handled consistently to comply with any applicable force and national information retention, classification and handling policies, standards or guidance

Scope of this policy

This document applies to all records in *any* formats created, received or maintained by staff in the course of carrying out their official duties. The policy applies to records in all formats:

- hard copy (i.e. paper records or files stored on or off site)
- electronic and digital, whether stored in the cloud or on social media, or on magnetic, digital, photographic and optical media, including network or removable drives
- emails created, received or maintained by staff of the force in the course of carrying out the functions of the force

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

What *are* records?

Records are both evidence of business activity and information assets in their own right. Their role as evidence in the transaction of business and their reliance on metadata (indexing tags) distinguish records from other information assets. Record metadata indicates and preserves context and apply appropriate rules for managing records.

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. 2016 (2nd edition)).

Although this is not an exhaustive list, records include:

- Documents (including written and typed documents, scanned, and annotated copies) such as:

a) Contracts, deeds, agreements, judgements and adjudications

b) Correspondence, reports and advice given and received

c) Memoranda, operating instructions, executive decisions, policies and procedures

d) Agendas, minutes, decisions, actions and outcomes of meetings

e) Registrations, appointments and announcements

f) HR personnel and medical files, Development Plans and Professional Development Reviews

g) Financial information, invoices, purchase orders, bank statements and monetary transactions

h) Intellectual property, patents and trademarks

i) Any other necessary documents, communications and information received by the organisation, or generated by the organisation, in the course of conducting its business

- Crime, custody and PNC records
- Witness statements
- Computer files (including word processor files, databases, spreadsheets and presentations)
- Electronic mail, text messages and tweets
- Diary records and pocket notebooks (PNBs)
- Police station ledgers, registers and convict or criminal lists.
- Fax messages
- Brochures and reports
- Web pages (Intranet and Internet)
- Forms
- Seized evidence (e.g. from mobile phones as well as physical documents)
- Digital (interview) recordings, audio and video tapes, including CCTV and BWV footage
- Microfiche and microfilm
- Maps and plans
- Photographs

Why records are important

As important documents, data sets or exhibits, records are retained to ensure that an

organisation can:

a) fulfill its legal and regulatory obligations

b) discharge its duties to its stakeholders, including customers and staff

c) conduct day-to-day business properly

Regardless of their storage media or location, the force will keep records that are complete, authentic, reliable, secure and accessible.

It will manage its records efficiently and cost-effectively throughout their lifecycle, in accordance with best practice, including legislative requirements and relevant industry standards, and using appropriate, interoperable, digital technologies with all necessary policy enforcement capabilities.

Police records management in a digital cloud world

Increasingly, police records are stored in hybrid environments because cloud computing enables controlled access to supersecure data centres over the internet on demand, for processing power, data storage and application software. These are rented on a "pay only for what you use" basis. Demand flexes with business need while a wider range of devices is supported, and updating and maintenance are simpler and automatic.

Police officers and staff are freed up to focus on their mission priorities, with intelligence and data at their fingertips, while their feet are on the street/beat. It eliminates time-wasting trawling through multiple information silos for what they need quickly, to get the job done.

This policy supports a more holistic approach to records, which de-siloes costly and time-consuming switching between multiple different and disconnected storage systems (or content repositories) to retrieve the desired information from them.

Since September 2017, police are permitted to store their records and information securely in "the cloud", for resilience, reliability and affordability, convenience and collaboration. The National Police Information Risk Management Team's decision to permit this was based on its strict standards which must be met before law enforcement agencies can move data to the cloud, as it ensures that information is held in a Police Approved Secure Facility. The National Enabling Programme's 1st Core Principle is "Cloud is good", which indicates the extent to which policing has now embraced the cloud computing model.

Whenever possible, supplier and partner compliance with the UK Government's G-Cloud Framework, the National Cyber Security Centre (NCSC) 14 Cloud Security Principles and the ICO Guidance on Cloud Computing is essential to safeguard force information assets including records. All three are aligned with ISO 27001 on information security. In addition, suppliers' and partners' should ideally align with the core services and relevant modules of the international MoReq2010® standard, whose best practices are be strongly encouraged during requirements gathering and system design stages and when the force expands or renews its technology estate.

Benefits of effective records management

Regardless of the storage media or location, the benefits of effective records management include:

- *Consistency, efficiency, continuity, productivity and security* of overall business management by:
    - supporting policy formation and decision making

- protecting force confidence in the lawfulness, quality and security of its records
- protecting the rights and freedoms of staff and the public
- facilitating consistent and equitable delivery of service

- *Information lifecycle managem ent supports the business* through systematic, cost effective and efficient application of controls to information, to maintain its evidential weight and protect its authenticity, availability and integrity.

- *Availability* of information in any format for business use, including lawful, authorised sharing with other enterprises. This underpins compliance with the College of Policing's Applied Professional Practice APP/MoPI Code of Practice; the Data Protection Act 2018, Freedom of Information Act 2000, Protection of Freedoms Act 2012, and other relevant legislation.

- *Reduces or eliminates costs* - through the proper control of the information, storage and volume of records, finding and managing information, and promotes best value in terms of human and space resources.

- *Risk management and mitigation* - by compliance with records management policy and standards and by enabling the provision of evidence of business transactions, thereby reducing vulnerability to legal challenge.

Risks of poor records management

Risks associated with ***not*** following good records management procedures include:

- inability to ensure that records are present, accessible, capable of being interpreted, trusted and maintained through time

- non-compliant relationships and contracts with third parties or suppliers whose support, systems or partnerships fail to meet applicable legal requirements and industry standards

- Health and Safety risks associated with the storage of large amounts paper incorrectly and / or unnecessarily (e.g. trip hazards, blocking exits and risk of fire)

- operational risks leading to lost court cases

- inability to comply with legal obligations or other regulatory requirements (e.g. MoPI, Data Protection, Freedom of Information, VAT rules etc.)

- possible critical incident occurring in Derbyshire, including but not limited to vulnerability to threats such as cyberattack, tampering or accidental deletion, malicious damage or viral contamination, or unlawful retention by a data processor after the data controller has withdrawn from a cloud service contract

General Principles

This Records Management policy, related best practices, and supporting guidance, incorporates the broad principles below, regardless of their storage media or location:

- Records that are complete, authentic, reliable, secure and accessible will be kept by the force and throughout their lifecycle those records will be managed in accordance with best practice, including legislative requirements, such as the six Data Protection principles:

    1. Processed lawfully, fairly and in a transparent manner in relation to the data subject (known as the lawfulness, fairness and transparency principle)

2. Collected for *specified, explicit and legitimate purposes* and not further processed in a manner that is incompatible with those purposes (known as the ***purpose limitation*** principle)

3. *Adequate, relevant and limited to what is necessary* in relation to the purposes for which they are processed (known as the ***data minimisation*** principle)

4. *Accurate* and where necessary, *kept up to date;* every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (known as the ***accuracy*** principle)

5. Kept in a form which permits identification of data subjects for *no longer than is necessary* for the purposes for which the personal data are processed (known as the ***storage limitation*** principle)

6. Processed in manner that ensures *appropriate security* of the personal data, including *protection* against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (known as the ***integrity and confidentiality*** principle).

- A *risk management*, project-based approach to the development and implementation of records management policy and standards will be followed.

- Recognised records management *standards* will be consulted and integrated into the Force Records Management Programme wherever appropriate (as detailed below). Examples include the Lord Chancellor's Code of Practice on the Management of Records under S46 of Freedom of Information Act 2000, International Standards Organisation (ISO) 15489, ISO 17799, ISO 9001, ISO 27001, MoReq 2010®, the National Cyber Security Centres 14 Cloud Security Principles, the British Standards Institution (BSI) BIP 10008, 0009, 0010 and 0025 and the Government Security Classifications. This is not an exhaustive list.

- Records management best practice recognises that a record can be in any format and has a defined *lifecycle*. A record also requires metadata to ensure that it is managed systematically.

- *Metadata* should be based upon a business classification scheme (such as the Police Service File Plan (PSFP – see below) and should stay with the record until the point of disposal when the record is no longer needed for business purposes.

- *Disposal* is governed by a retention (or disposal) schedule that sets out the period for retaining a given record type. During or at the end of the retention period the record is reviewed and a disposal decision is made, which might be to retain the record for a further period of time, pass the record to another organisation, for example The National Archives, or to destroy the record securely without possibility of restoration.

The Force Records Management Programme below is based on this policy and complies with all relevant legislation and codes of practice including the Police Authorised Professional Practice (APP) and the Management of Police Information (MoPI) 2010.

Roles and responsibilities (Governance)

Regardless of their storage media or location, the force has a corporate responsibility to maintain its records and record keeping systems in accordance with its legal obligations and best business practice.

All police officers and staff have a responsibility to comply with this policy and practise good

records management in their daily operations (see further below).

Overall governance for records management is shared across a number of specialist roles and responsibilities including executive and senior management, records management professionals, and systems specialists/administrators. They are:

- Executive Management – the Chief Constable has overall responsibility for Records Management Policy and standards and is also the Force's Data Controller.
    - The Chief Constable is represented by the Deputy Chief Constable (DCC), who chairs the Strategic Information Management Board, on which the Head of Information Management also sits. The Deputy Chief Constable (DCC) is also the Force Senior Information Risk Owner (SIRO).
    - Chief Officers have a responsibility to champion the application of the policy and its related guidance and standards force wide.
- Below Executive level, Information Asset Owners and their designated Information Asset Assistants are responsible for the business decisions regarding their records and any decisions to implement new systems or formally decommission any that are no longer needed or used within their business area. They are also responsible for the appropriate safeguarding or disposal of the data within those systems. Decommissioning must be formally recorded and ratified by the Strategic Information Management Board (SIMB). The full range of IAO responsibilities is covered in more detail in the IAO Policy.
- The Force Records Manager is responsible for the development, implementation and maintenance of the records management best practices and guidance that underpin the Records Management Policy. These are crystallised in the Records Management Programme (details below). When required, the Force Records Manager advises the Force Executive and Senior Management above on records management matters.
- When planning at pre-programme or pre-project stage, new programme and project managers in both technology and business areas have a responsibility to ensure that new systems, processes and changes are designed and developed by default to comply with the criteria in the Information Management Business Considerations document, which is revised periodically. This should be done in full consultation with the force's data protection, information security and records management subject matter experts.
- The Information Management Business Considerations document provides guidance on a range of essential inclusions in new or planned systems which ensure "good design by default". It is revised by the Data Protection Team and the Force Records Manager periodically as new technologies or business changes demand.

Forcewide, all police officers and staff have a day to day operational responsibility for any documents and records that they create or use. This responsibility is defined in law and is included in terms of employment. In particular, all police officers and staff must:

- ensure that records are classified and handled in accordance with the access and security environment and are protected from unauthorised disclosure (need to know principle). See the Access and Security section below for more details
- implement the Records Management Policy and associated best practices to the best of their knowledge and ability
- ensure that records for which they are operationally responsible, regardless of their storage media or location, are:

- accurate, maintained and disposed of in accordance with the force's records management policy, best practices and standards outlined or referenced in this document

- maintained in compliance with Data Protection principles and other applicable local requirements

- marked and handled correctly according to the force's Information Classification and Handling Policy (see Access and Security section below)

- recorded and stored in the appropriate format and location

- securely and safely stored when decommissioning or refurbishing police premises, offices, floors, or storage areas (see Decommissioning of police premises section below)

Strategic Information Management Board

The Board has strategic oversight of areas of Information Management within Derbyshire Constabulary and its members represent a broad cross-section of the force's business interests.

It seeks to maximise the benefits of operational information and exploit its lawful use to support effective decision making, and identifies and pursues the options with the best value for money.

It also seeks to develop an informed culture within the force that supports the use of innovation in technology and data quality improvement, whilst taking account of the threats to its information assets.

In particular, with regard to records management, the Board:

a) oversees delivery of the force's Information Management and Record Management Strategies and monitors progress through regular review of the supporting implementation plans.

b) ensures that the force achieves and maintains compliance with the NPCC Community Security Policy and relevant national information security standards, the Code of Practice for the Management of Police Information (MOPI) and associated guidance

c) ensure that the force achieves and maintains compliance with its statutory obligations, including those which arise from GDPR and the Data Protection Act 2018, Freedom of Information Act 2000, other relevant legislative and associated records management responsibilities

In practice, the Board ensures clear lines of accountability for records management by ensuring that a senior manager:

i) is responsible for coordinating, publicising and monitoring implementation of the records management strategy and reporting on a regular basis to the Head of Information Management

ii) monitors and reviews systems in place for records management as part of an ongoing force service improvement mandate

iii) seeks independent assurance that an appropriate and effective system of managing records is in place

iv) formally records all key records management related decisions, including but not limited to, formal sign off on decommissioning of systems after risk assessment and due diligence by its IAO and the lawful, timely disposal of the data from those decommissioned systems

Information Asset Owners (IAOs)

Ownership of the business record normally lies with the Head of each business area, *who automatically becomes the Information Asset Owner* for their business area upon their appointment. Where no clearly defined business owner of a record exists, ownership for disposal will default to the Force Records Manager until the Strategic Information Management Board (SIMB) identifies and appoints a suitable Information Asset Owner.

Information Asset Owners and their Information Asset Assistants are champions for information management and data protection. They are accountable and responsible to the force Senior Information Risk Owner (SIRO).

Regardless of their records' storage media or location, and in accordance with the Information Asset Owner Policy, IAOs and/or IAAs will:

i) collaborate with the Force Records Manager to define any service levels where policy and standards are not explicit

ii) be responsible for records management and ensure that all staff are involved in the implementation of the Records Management Policy and Programme, through internal communication, profile raising, publicity and by ensuring appropriate resources, training

iii) ensure that during the planning and design of new systems, information management principles and considerations are designed in by default at pre-inception, requirements gathering, or other project inception stages

iv) ensure the formal decommissioning of any systems (physical or digital/cloud-based) which are no longer needed or used within their business area and that the formal decision to decommission is made and recorded by the Strategic Information Management Board (SIMB)

v) 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 schedule must be incorporated into the Statement of Requirements for all future procurement of electronic data management applications

Information Asset Assistants (or Supervisor equivalent for day to day maintenance, monitoring)

Each business area will have a designated Information Asset Assistant who deputises for the Information Asset Owner and when required, and works to their guidance. Regardless of the storage media or location, IAAs will be responsible to:

i) develop, operate and communicate records management procedures, covering both electronic/digital/cloud-based and hard copy media

ii) complete the Information Asset Register for their business area, where necessary with the assistance of the Force Records Manager

iii) ensure records are fit for purpose, in the appropriate recording formats, and comply with Records Management Policy and standards

iv) quality assure records management processes and procedures

v) ensure that staff are aware of their personal responsibilities for record keeping

vi) ensure appropriate staff training to maintain a high standard of skills and competence.

The Information Asset Owner Policy should also be consulted for more detailed information about both Information Asset Owners and Information Asset Assistants.

Force Records Manager

The Force Records Manager will have the following responsibilities, regardless of any record's storage media or location:

i) pursue, as far as is reasonable, practical, and at acceptable cost, a Records Management Programme that complies with key records criteria (listed below) and which safeguards the protection, retention or destruction of all associated records in a records chain i.e. digital *and* physical records whether stored in the cloud, social media, email or physical media, that are related to a nominal or occurrence in the designated records management system

ii) be the records management single point of contact (SPoC) for Information Asset Owners and Information Asset Assistants and provide them with all necessary support and guidance to discharge their information management roles effectively and lawfully

iii) assist Information Asset Owners to plan and design or decommission any systems within their business area by ensuring that those systems embed by default a range of strong information management considerations and principles to protect the force and safeguard public confidence

iv) produce a Records Management Policy with related best practices and supporting guidance, update them when necessary, and ensure that they are relevant to the needs and obligations of the force, by consultation and assessment against external standards

v) produce a Review, Retention and Disposal Policy and schedules, ensure that it is implemented, and update it when required

vi) produce and maintain an Information Asset Register, in conjunction with Information Asset Owners and/or Information Asset Assistants

vii) producing a list of force vital records that has been validated by the Information Asset Owners of business areas and ratified by the Business Continuity Steering Group

viii) work closely with the Business Continuity Manager/Officer to ensure that a business continuity plan is in place to provide protection for records which are vital to the continued functioning of the Force, and covering the records of the Information Management Department. Business Continuity planning is covered in more detail below, in the Preservation of records section.

ix) conduct and recommend records management training needs analyses for each business area when triggered (see Learning and development section below)

x) maintain strong records management relationships with internal and external stakeholders, including audit and management team

xi) ensure that management teams supervising divisional/department records management have the necessary skills and competencies

xii) manage and monitor the storage conditions of all records on-site and off-site including contract or deposit-based storage services (e.g. in warehouses or historical (public) archives) or in the cloud, in keeping with best practices in the UK Government's G-Cloud Framework, the National Cyber Security Centre (NCSC) 14 Cloud Security Principles and the ICO Guidance on Cloud Computing, as well the guidance in MoReq2010®

xiii) monitor individual and force compliance with the Records Management Policy, best practices and any relevant standards, regardless of storage media or location

Records Management Programme

Regardless of their storage media or location, the force will manage its records in an integrated and co-ordinated way:

- to ensure that they remain credible and authoritative throughout the record lifecycle
- to be compliant with BS ISO 15489-1:2016 and, where applicable, MoReq 2010®
- to be complete, authentic, reliable, secure, usable and have integrity
- to ensure that records systems incorporate strong compliance by design and default with the Information Management Business Considerations document and when necessary or appropriate, MoReq 2010®, the UK G-Cloud Framework and the National Cyber Security Centre's 14 Principles on Cloud Security

To achieve this, the Records Management Programme will satisfy the following records criteria:

Authenticity

It must be possible to prove that records are what they purport to be, that their integrity is demonstrably intact and it must be possible to identify who created them. Where information is added, an audit trail of the added information will be created.

Accuracy

Records must accurately reflect the transactions that they represent.

Integrity

Records must be securely maintained to prevent unauthorised access, alteration, damage or removal. They will be stored in a secure environment, and protectively marked in accordance with the requirements of the Government Security Classification Scheme (previously Government Protective Marking Scheme).

Usability

Records must be readily available and sufficient in content, context and structure to provide adequate authenticated evidence of the relevant activities and transactions. This includes the accessibility and use of electronic records for as long as required (which may include their migration across systems); and the ability to cross reference electronic records to their paper counterparts in a mixed environment.

The term "readily available" is not the same as immediately available. The speed at which records can be retrieved depends on where, how and in what format they are stored. Files or tapes may have to be retrieved from offsite archive facilities, which may take time.

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

Review

Records must be reviewed and disposed of promptly in accordance with the Records Retention Schedule and the NPCC National Retention Tables, which can be found in the force Review, Retention and Disposal (RRD) Policy. An audit trail will be kept.

Evidential weight

The intelligent application of records management standards and principles above should result in fewer, higher quality records, which are more useful as evidence and a reliable source of information on which to base decisions.

The force will seek to comply with standards such as BS 10008:2014 – Evidential Weight and legal admissibility of electronic information and BIP 0025:2002 – Effective Records Management.

Best practices

To ensure by strong design and default principles that force records are complete, reliable, authentic, secure and accessible, regardless of their storage media or location. To achieve this the following best practices must be followed

a) Records must be categorised, when necessary or appropriate, in accordance with the force file plan which should be broadly consistent with the Police Service File Plan (PSFP)

b) Records must be stored, and where appropriate, segregated, so as to provide adequate protection against unauthorised access or damage or other threats

c) Records must be promptly rectified in the event of error and recipients to whom incorrect or inaccurate data has been disclosed or shared must be informed of the error promptly in order to facilitate rectification

d) Records must be readily available to meet operational need and legal obligations. A list of vital (critical) records for business continuity purposes will be maintained, and reviewed and updated periodically

e) Records must be disposed of promptly in accordance with the Retention (Disposal) Schedule and an audit trail kept

f) Records management systems must provide an auditable trail of records transactions from creation through to ultimate disposal

g) Business decisions on obsolete systems, no longer used due to upgrade or data migration, must be presented for formal approval to decommission by the Strategic Information Management Board (SIMB)

h) To minimise the risk of records being overlooked during a migration exercise, electronic files should not be stored on local disks or removable media unless there is a genuine business need (e.g. sealed master disks for use in court cases)

i) Where files are created and/or updated using mobile or portable computing devices (e.g.laptops or MDTs), 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.

j) Records stored in cloud based systems must be designed and developed by default for information compliance and assurance in full compliance with the Information Management Business Considerations document, with early consultation of the force's data protection, information security, and records management subject matter experts, whenever new systems, processes and changes are introduced to the force. Consideration should also be given to the UK G-Cloud Framework, the National Cyber Security Centre's 14 Principles on Cloud Security, and MoReq 2010®.

In particular, new programme and project managers in both technology and business areas have a responsibility to:

- ensure that, where necessary, terms and conditions are in place to protect, secure and safeguard the lawfulness of any Derbyshire Constabulary's data processed by third parties, in particular by considering:

- the guidance in MoReq 2010®, The UK G-Cloud Framework and the National Cyber Security Centre's 14 Principles on Cloud Security when system designing and assessing the adequacy of storage facilities. For MoReq 2010®, particular attention should be to the Information Model and Data Structures (chapter 14), general Functional Requirements, Non-functional Requirements (chapter 12), and Electronic Components of records (chapter 301), as well sections on Model Metadata, APIs, GUIs.

Note: even though this is not yet a formally ratified international industry standard, it represents the future and developed from its predecessors for the changing digital world and national of a record. Accordingly, it contains sensible requirements for suppliers and systems planners and designers. See Glossary.

For high level *functional* requirements, particular note should be taken of the following, all of which are defined and more fully explained in MoReq 2010® itself:

- a user and group service
- a role service
- a classification service
- a record service
- a metadata service
- a disposal scheduling service
- a disposal holding service
- a searching and reporting service
- an export service.

Each service may be implemented individually or several services may be bundled together.

For high level *non-functional* requirements, particular note should be taken of the following, all of which are defined and more fully explained in MoReq 2010® itself:

• performance	• availability
• scalability	• reliability
• manageability	• recoverability
• portability	• maintainability
• security	• supported
• privacy	• warranted
• usability	• compliance
• accessibility	

For the electronic components of a record, the following attributes are essential, all of which are defined and more fully explained in MoReq 2010® itself:

- *Discreteness* − must have its own separately identifiable content
- *Completeness* − in combination with the other components of the record, must comprise a whole atomic record which is not dependent for its evidential worth on external resources
- *Immutability* − once created, the content must not change over time, or be able to be erased, until it is destroyed or deleted by the system
- *Destructibility* − the content must be able to be deleted, either automatically or with confirmation, in response to its destruction in the system
- *Transportability - may be transferred from an originating system to another receiving system for interoperability and long -term preservation*

Record Creation

Each operational/business area must have in place an adequate system for documenting its activities. This system must take into account the legislative and regulatory environments in which the force works.

Records, databases, and records management systems should be registered on the Force Information Asset Register and their owners in the Information Asset Owners Master List, both of which are maintained by the Force Records Manager.

Regardless of the storage media or location, the force must have in place controls to ensure the record is created on the appropriate form or database and is assigned the relevant classification, naming convention and protective marking.

Each operational/business area must notify the Force Records Manager of any creation or intended creation of new databases for assessment and inclusion in the Information Asset Register.

Each notification for an intended creation of new database(s) for assessment must be submitted in business case format to the Force Records Manager.

Each new system or database of records must be notified to the Force Records Manager for registration on the Information Assets Register and Information Asset Owners Masterlist.

Registration

The Force Records Manager must identify, monitor and action those records that are appropriate for registering, remaining on the Force Information Asset Register and those that are not, regardless of their storage media or location.

The Force Information Asset Register is its master inventory of information assets, which Information Asset Owners, or their Information Asset Assistant(s), should be revising on an ongoing basis, with formal consolidations every two years (biennially). This will normally be completed with the guidance and assistance of the Force Records Manager. If updates are tackled on a systematic and regular basis, biennial consolidations are easier, simpler and quicker to complete.

If a file, record or group of records (databases) due for destruction is known to be the subject of a request for information (e.g. Inquiries Act documents, Freedom of Information or Subject Access Requests), destruction should be delayed until disclosure has taken place or, if the force has decided not to disclose the information, until the complaint and appeal provisions of the Freedom of Information Act (FoIA) 2000 or other relevant legal causes have been exhausted.

The Force Records Manager is responsible for all file/document registration activity including alterations and destructions/disposal, regardless of their storage media or location.

The Force Records Manager is responsible for conducting periodic review and evaluation of systems registers to ensure accuracy and completeness.

The Force Records Manager is responsible for ensuring that all registered files, records or groups of records (databases) are available for those with authorised access.

Files, records or groups of records (databases) remain on the Information Asset Register in line with the College of Policing's Authorised Professional Practice/ MoPI 2010.

Classification and Indexing

Classifying and indexing information is a vital discipline. In this context, classification means indexing with essential metadata (see below), to enable effective and rapid retrieval and which permits logical organisation for ease of identification, finding or isolation. Classification does not mean protective marking or information handling from a security perspective, which is discussed separately in this document.

Indexing can be done manually or automatically generated. The function of an index or referencing system is to provide the user with an efficient means of tracing, finding or isolating information. Indexing and referencing requirements apply to all records, regardless of their storage media or location.

Good practice here dictates a functional rather than an organisation structural approach. At the top level the classes cover the key functions for which the organisation is responsible. Below are the activities that define each function and the transactions or processes comprising them.

The force may use a record Police Service File Plan (PSFP) classification system where necessary or appropriate, based on all business activities which generate records, and both categorise and index those records to facilitate in a systematic and consistent way:

a) linkage between individual records that collectively give a continuous record of activity

b) retrieval of all records relating to a particular function or activity

c) assessment of security protection and appropriate access for sets of records

d) distribution of responsibility for management of particular sets of records

e) evaluation of appropriate retention periods and disposition actions for records

f) immediate establishment of the presence or absence of information on a given subject

g) identification and location of relevant information within a set of records

h) logical grouping together of similar information on subjects

Metadata

As well as the content, records should contain, be linked to, or associated with, metadata – descriptive and technical documentation about the file or document such as:

i) how, when and by whom it was received, created, accessed and/or modified and how it is formatted

ii) intended disposal of electronic records should be included in the metadata when the record is created.

MoReq2010® also contains helpful guidance on metadata and its value for data export and interoperability in chapter 7. International standards on Metadata also apply: ISO 23081:1-3.

Records storage

Regardless of storage media or location the Force Records Manager will supervise and ensure that any record can be tracked (the movement and location) and monitored so that:

i) storage is secure for the relevant retention period, in a designated physical or cloud-based location, and limited to the minimum time necessary to achieve its purpose

ii) authorised retrieval is easy at any time, and

iii) an auditable trail of record transactions is available, and

iv) lawful and secure disposal at the relevant review point is possible, when no longer required for the conduct of current business, or

v) appropriate environmental or technical controls are in place to prevent damage or degradation to the records

vi) equipment and facilities used for current records storage is fit for purpose and safe from unauthorised access, and meeting standards such as the UK G-Cloud Framework and the National Cyber Security Centre's 14 Principles on Cloud Security where cloud storage is adopted. For physical records, compliance with fire regulations and reasonable protection from water, rodent or other damage is imperative, while permitting the maximum approved accessibility to the information, commensurate with its frequency of use.

Preservation of records

Long term preservation of physical records

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):

a) adverse temperatures

b) fluctuations in relative humidity

c) exposure to light

d) pest infestations (insects or vermin)

e) mould

a) pollution

g) stability, acidity or impurity of the paper

h) quality of the storage wallets, folders and boxes used

i) incorrect handling

The Records Manager will work with Assets and Information Security, as appropriate, to ensure that equipment and storage onsite and offsite facilities for current records are 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. External offsite facilities such as Iron Mountain may be subject to PASF accreditation.

Exhibits

Exhibits will be stored in accordance with the force Evidential Property Policy.

Preservation of electronic records

Preservation of electronic / digital records is a more complex challenge, known as digital obsolescence. Physical storage media such as CD ROMs need both hardware on which to play the medium (CD / DVD drives) *and* software to read the data on the medium, in order to present it to the user in a comprehensible way (e.g. a compatible version MS Word etc.). Absence of any one of these three conditions makes the record irretrievable.

If digital obsolescence has already occurred, remedy of the situation is usually extremely expensive, even if it is at all possible.

To avoid digital obsolescence the force is increasingly moving to cloud-based storage in data centres or on dedicated and networked servers (e.g. O365/Azure). Data is migrated onto these servers with the necessary supporting (rendering) software as the technology advances. This is particularly effective where the information contained within records is more important than the way that information is displayed.

Where it is not already being utilised, and it is appropriate to do so, consideration should be given to using secure cloud-based storage options such as O365 and Azure and ensuring that facilities are fully compliant with the UK G-Cloud Framework and the National Cyber Security Centre's 14 Cloud Security Principles. (see MS Azure's documents on Compliance Offerings and the 14 Cloud Security Controls for the UK Cloud.)

During records migration across or through changes in technology, the force must 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.

Business continuity planning and responsibility

All servers controlled by IT systems are backed-up, including by definition, cloud-based applications. However, the information may not necessarily be in a format that can be swiftly accessed following a disaster. An IT 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. Cloud-based applications would likely be a part of this group.

It is the responsibility of each department to ensure that their business continuity and disaster recovery plans provide adequate contingencies (Recovery Time Objectives or RTOs) for the IT systems that the department owns and/or uses, if they are not covered by the overall Force IT Service Continuity Plan.

If business areas place electronic information outside of the force's IT infrastructure (e.g. in non-IaaS contracts (IaaS = Infrastructure as a Service)), it is the responsibility of that business area to ensure that the information is backed-up, secure, and recoverable in the event of a disaster. Any back-ups will restore the system to a given point in time. It is the responsibility of business owners to ensure that all processes applied to the system between the back-up being captured and restored are re-applied as soon as possible. See the UK G-Cloud Framework and the National Cyber Security Centre's 14 Cloud Security Principles.

Scanning

Scanning of paper records is time-consuming and should only be undertaken when there is a genuine business need, such as the need to:

a) create space by disposing of the original paper record, or,

b) 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 Information Services to ensure that there is sufficient capacity within the IT infrastructure (including cloud-based storage) 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. Records need also to be properly metadatised for rapid, accurate and timely retrieval or authorised disclosure.

Where scanning results in the disposal of the original record, care must be taken to adhere to the scanning standards set out in BS 10008:2014 (Code of Practice for evidential weight and legal admissibility of electronic information).

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

a) scanned image of sufficient quality cannot be obtained

b) scanned image requires significant enhancement

c) record has physical amendments that have not been captured (e.g. pencil annotations that do not show up properly, or Post-It™ notes)

d) fraud is suspected

e) legal reason(s) for retaining the original (e.g. required by contracts)

f) scan is of an exhibit (e.g. a hate-mail letter)

Originals of scanned, non-Derbyshire Police records should 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.

Review, Retention and Disposal

Regardless of the storage media or location, review and disposal procedures will ensure that information held by the force is held lawfully and for the minimum time necessary to achieve its purpose. They will also prevent forces being overloaded by the volume of information captured and recorded. Particular attention should be given to cloud-based storage to avoid unlawful retention or accidental or premature deletion. The UK G-Cloud Framework and the National Cyber Security Centre's 14 Cloud Security Principles should also be applied when appropriate.

To effectively manage risk, the force's controls and procedures are aligned with legislative and operational governance including the Data Protection Act 2018, Limitation Act 1980, and Criminal Procedures Investigation Act 1996, the College of Policing's (2014) Authorised Professional Practice/ MoPI, as well as, when appropriate, the Protection of Freedoms Act 2012.

The standard procedures below enable the force to make informed, accountable decisions about records retention or destruction/disposal:

i) records should be retained only for as long as they are required and until their scheduled disposal, according to their operational, legal, administrative and historical evaluation

ii) once the decision is made for destruction/disposal of records they should be destroyed/deleted in as secure a manner as necessary for the level of confidentiality or security markings they bear. The force's Information Classification and Handling Policy and the Government Manual of Protective Security and National Policing Community Security Policy specify requirements for handling and disposing of classified material

iii) a record of the destruction/disposal of records (e.g. destruction certificate), showing their reference, description and date of destruction/disposal should be maintained and securely preserved

iv) records will be kept on file of every review undertaken, irrespective of whether it resulted in any alterations or destruction/disposal, for audit purposes and in accordance with MoPI

v) records will be disposed of or archived in line with APP Authorised Professional Practice / MoPI 2010 or the appropriate functional legislative guidance (e.g. Finance, Occupational Health, HR, etc)

vi) records must be destroyed/deleted in such a way that the information they contain cannot be re-constituted by any commonly known or practised methods

vii) electronic / digital records should be retained and preserved on or in media that permit reliable access, data migration and/or auditable system modifications

viii) records, irrespective of their format of creation, must remain accessible up to the point of disposal by maintaining an effective means of accurate reproduction, in a timely manner and without compromise to the the record

Please see the Force Review, Retention and Disposal Policy for further information and seek guidance from the Force Records Manager when necessary.

Retention (Disposal) Schedule

The initial minimum retention period for most policing records is 6 years from the date of creation. In line with a formal review schedule, on reaching this date, all policing records must be reviewed to ensure that they can continue to be held lawfully and remain both relevant and accurate, regardless of their storage media or location. Any non-policing records must also have defined retention periods which are strictly adhered to.

Ownership and responsibility for setting, reviewing and updating the disposal schedule for policing information will be with the Force Records Manager and the Strategic Information Management Board, in line with the College of Policing (2014) Authorised Professional Practice / MoPI 2010.

The force Review, Retention and Disposal Policy (RRD Policy) contains the current retention schedule as approved by Chief Officers and sets out the review, retention and disposal periods for policing records held by the force in line with national or regional legal and operational requirements (NPCC, 2017/18) and the College of Policing (2014) Authorised Professional Practice / MoPI 2010.

In evolving areas of ambiguity, or which are felt to be insufficiently clearly addressed at national or regional levels, the Force Records Manager may add specific records retention duration periods to the local Derbyshire schedule, where they assist with operational clarity for Information Asset Owners and Assistants.

Access and Security

The legal and business environment in which the force operates establishes broad principles on access rights, conditions and restrictions.

Access and security vigilance applies at all times, regardless of records storage media or location. For cloud based storage and systems, compliance with the UK G-Cloud Framework and the National Cyber Security Centre's 14 Cloud Security Principles is essential.

The Government's Security Classification (GSC) applies to all the Derbyshire Constabulary records and information and will be complied with at all times.

Restricted records will be identified only where specifically required by business need or the business environment.

Restrictions will be imposed for a specified period to ensure that the additional security controls required for these records is not enforced for longer than required.

The data controller and business process owner will assign individuals access status in accordance with the Force Information Security Policy. The monitoring and mapping of user permissions and functional job responsibilities is a continual process, as defined in the Force Information Security Policy.

De-commissioning of police premises

The Information Security Policy on Clear Desks and Clear Screens will be strictly adhered to by all force officers and staff. That policy is further reinforced by the force Records Management Policy to:

- protect computer screens, removable or portable media, and
- physical files, boxes or paper records

from unauthorised opportunistic consultation if left unattended, or exposure to loss, theft or unauthorised removal, during business hours, while off duty, or during refurbishment, redecoration or reorganisation.

Prior to the de-commissioning of police premises, the police officer(s) in charge or their authorised delegate, and their staff, are collectively responsible to protect the digital and physical security of force information in all its formats, and during its transit to a new or temporary secure location.

De-commissioning of police premises will include an assessment from Police Search Advisor (POLSA) in order to seek assurance of no legacy record being exposed as a security risk.

Office, floor or room refurbishment, redecoration or reorganisation

Similarly, during office, floor or room refurbishment, redecoration or reorganisation, the police officer(s) in charge or their authorised delegate, and their staff, will strictly adhere to the policies cited above.

All files and records regardless of format will be securely stored in a safe location before, during and after any office, floor or room refurbishment, redecoration or reorganisation, or securely handled in transit when it is moved or transferred to a new location.

Under no circumstances should removable or portable media or physical files, boxes or paper records be left unattended or exposed to unauthorised opportunistic consultation, loss, theft or removal, while any temporary work is undertaken.

Learning and Development

The force will ensure all staff receive appropriate and timely training, based on training needs analysis, using appropriate training products.

A force training needs analysis will be conducted at regular and appropriate intervals according

to need.

The force training needs analysis triggers will include:

- new records management staff
- movement in staff at any level
- change in functions and responsibilities
- change in policy and/or standards
- introduction of a new system(s) including any cloud-based processing, storage or applications
- change in national or legislative records management environment
- security or data breaches

The Force Records Manager will be responsible for conducting and recommending records management training needs analyses for each business area.

The Learning and Development Department will be responsible for co-ordinating, reviewing and recording training activities.

Audit and Compliance

Where an internal force audit or quality assurance (QA) review is conducted, compliance with the force records management policy and guidance must be included as an integral part of the review process. The force Information Management Department has responsibility for auditing and ensuring compliance, which will include scrutiny of cloud-based storage and security, based on the UK G-Cloud Framework, the National Cyber Security Centre's 14 Cloud Security Principles and where appropriate, any relevant provisions in MoReq 2010®.

Independent audits will be conducted periodically, as appropriate.

Audit trails must be:

- provided for all records and documents
- kept securely and available for inspection by authorised personnel
- managed as critically important to the organisation. Claims of compliance may be discredited if the audit trail is not treated correctly and cannot be interpreted unambiguously.
- secure. If an audit record can be maliciously or inadvertently altered then the whole audit trail may be discredited.

Audit trails must include a record of all relevant occurrences. 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.

Law Enforcement audit trails under the Data Protection Act 2018 are called logging. They must be kept for any IT database or system or automated processing and internal processing as a safeguard against inappropriate access or disclosure. The activities on which they focus are:

- Collection
- Alteration
- Consultation
- Disclosure
- Combination
- Erasure

Appeals Process

Appeals will be directed to the Head of Information Management for initial assessment and due process before reporting to the Strategic Information Management Board (SIMB).

Appendix 1

Records Management Glossary

Access	The availability of, or permission to consult, records.
Accountability	The principle that organisations and individuals are required to account to others their actions. Government departments and agencies must be able to account for their actions to the appropriate regulatory authority.
Appraisal	The process of evaluating an organisation's activities and records to determine which records should be kept and for how long, to meet the needs of the organisation, the requirements of Government accountability and the expectations of researchers and other users of the records.
Archive (n)	The physical place where archives are managed.
Authentic	An authentic record is one that can be proven to be what it purports to be, to have been created or sent by the person identified and created or sent at the time purported (BS ISO 15489: 2001).
Business recovery plan	A document which sets out the measures to be taken to minimise the risks and effects of disasters such as fire, flood or earthquake etc. and to recover, save and secure vital records should a disaster occur. It should include operational measures that enable the re-start of the business.
Classification system	The process of devising and applying schemes based on the business activities which generate records, whereby they are categorised in systematic and consistent ways to facilitate their capture, retrieval, maintenance and disposal. Classification includes determining document or file naming conventions, user permissions and security restrictions on records (BS ISO 15489: 2001). In broad terms it is the process by which records are categorised or grouped into retrieval units, whether by function, subject, or other criteria.
Clear Desk Policy	A force Information Security Policy reinforced by the force Records Management Policy to protect computer screens, removable or portable media, and physical files, boxes or paper records from unauthorised opportunistic consultation if left unattended, or exposure to loss, theft or unauthorised removal, during business hours, while off duty, or during refurbishment, redecoration or reorganisation.
Client manager	An officer of the Public Record Office responsible for giving advice and guidance to a group of government departments and agencies, to provide for the timely and effective appraisal, documentation and accessioning of departmental records.
Compliance	Fulfilling legal and regulatory requirements.
Cloud, Cloud Computing, Cloud-based storage	Applications, data storage or processing power available over the internet to an end-user or subscriber who pays a fee for one or any mix of these services from a provider, in one or more of three forms: *Software as a Service (SaaS)* – least subscriber control; *Platform as a*

	Service (PaaS) – little or no subscriber control; *Infrastructure as a Service (IaaS)* – total subscriber control). Cloud services are typically services or utilities rented online on demand, on tap. They also avoid the need for costly and time-consuming upgrades because they update online automatically. Cloud security standards should always be applied, based on the UK G-Cloud Framework, which itself is based on the National Cyber Security Centre's 14 Cloud Security Principles.
Current records	Records necessary for conducting the current business of an organisation.
Data controller	This is the person (an individual or a corporate entity such as a company) who determines why, as well as how, personal, data are to be processed. It is their duty to ensure that the collection and processing of any personal data within the organisation complies with the data protection principles.
Data processor	This is any person (other than an employee of the data controller) who processes the data on behalf of the data controller. Data processors must have a written contract in which the data controller defines how personal data, including sensitive personal data, is to be processed and what security measures will be appropriate. Although the data processor must, of course, observe the terms of the contract, the data controller retains full responsibility for the actions of the data processor.
Data processing	The systematic performance of operations upon data (facts without structure or context) such as handling, merging, sorting and computing, refers specifically to processing business data.
Data subject	The person who is the subject of the personal data. To count as a data subject the person must be living and capable of being identified from the data or other data in or likely to come into possession of the data controller.
Digital	When applied to information, documents etc. information store in a form, based not on human readable symbols but on a binary encoding, which can be manipulated by computers (and thereby made readable by humans).
Digital Continuity	The need to be able to use information in the way you need to for as long as is necessary, and certainly in years to come. It is about both durability and usability and is part of any business as usual process. We need to still be able to access and trust it (preserved accuracy and quality, uncontaminated / unaltered, etc).
Digital Obsolescence	As information gets older there is an increased risk that users cannot open or work with it due to hardware, software or file format obsolescence, decay or other kinds of poor data management including the loss of context or meaning or trust in its authenticity or integrity. Digital continuity planning and periodic risk assessments (for example, through early Information Management engagement during the planning and procurement of new systems, or migration of content during upgrades) will help mitigate or eradicate the likelihood of digital obsolescence.

Disposal	The implementation of appraisal and review decisions. These comprise the destruction of records and the transfer of custody of records (including the transfer of selected records to an archive institution). They may also include the movement of records from one system to another (for example paper to electronic).
Disposition	A range of processes associated with implementing records, retention, destruction or transfer decisions which are documented in disposition authorities or other instruments.
Document	A structured unit of recorded information, published or unpublished, in hard copy or electronic form and managed as a discrete unit (BS ISO 15489:2001). A document becomes a record when it forms part of a business transaction and is linked to other documents relating to that transaction or process.
Documentation	Facts about a record keeping system, including its component parts and a manual of instruction detailing rules for use and maintenance of the system.
Electronic records	Records where the information is recorded in a form that is suitable for retrieval, processing and communication by a digital computer.
File	An organised unit of records accumulated during current use and kept together because they deal with the same subject, activity or transaction.
Historical record	Anything recorded prior to the date that the College of Policing's (2014) Authorised Professional Practice: MoPI came into effect.
Information Asset Register	The Force's master inventory of information assets, which Information Asset Owners, or their Information Asset Assistant(s), should be revising on an ongoing basis, with formal consolidations every two years (biennially). This will normally be completed with the guidance and assistance of the Force Records Manager. If updates are tackled on a systematic and regular basis, biennial consolidations are easier, simpler and quicker to complete.
Information Survey	A comprehensive gathering of information about records created or processed by an organisation.
Integrity	The quality which when present means that the record possesses a verifiably incorruptible data/content and can identify the intellectual qualities of information that make it authentic.
Life cycle	An approach to viewing the records management through a lifecycle model. It divides the record five major phases of existence – creation, distribution, use, maintenance and disposal. As part of the disposal it may enter into the archive or be destroyed.
Metadata	Descriptive and technical documentation to enable the system and the records (that are described) to be understood and to be operated efficiently and to provide an administrative context for the effective management of the records.
Microform	Records in the form of microfilm or microfiche, including aperture cards.

Migration	In this context, it refers to the movement of data from one medium or system to another while maintaining the records' authenticity, integrity, reliability and usability.
MoReq2010®	The newest and most far reaching international functional specification published to date that defines how compliant records systems should operate and interoperate. While building on the foundational approaches of internationally recognised standards in records management, such as ISO 15489, ISO 23081, ISO 16175, and its predecessor MoReq2, MoReq2010® goes beyond any of these in its scope, definition and ambition.
National Cyber Security Centre	14 Principles on Cloud Security – a comprehensive set of considerations when moving to cloud storage or systems
Operational area	A unit, division or department within government department or agency with responsibility for a particular function.
Paper records	Records in the form of files, volumes, folders, bundles, maps, plans, charts, etc.
Personal Data	Factual information and expressions of opinion about, and any indications of anyone's intentions in respect of, living individuals who can be identified from that data or other data in the possession of, or likely to come into the possession of, the Data Controller. There are five categories of personal data: - **Category (a)** Information being processed by means of equipment operating in response to instructions given for that purpose, for example a database or a system with search capabilities which enables information about individuals to be identified and retrieved. **Category (b)** Information recorded with the intention of being so processed. **Category (c)** Information that is not processed automatically but is recorded as part of a "relevant filing system" or with the intention that it should form part of a relevant filing system. A relevant filing system is one in which particular information about specific individuals can be readily retrieved. The internal structure of the files is therefore relevant. Any system whose primary purpose is to hold information about individuals and comprises files with an internal structure or referencing system that facilitates retrieval of specific information about those individuals falls within this definition. **Category (d)** Records relating to health, education, social work and housing that were previously subject to data subject access under other legislation. There is a statutory definition at section 68. **Category (e)** Recorded personal information that does not fall into any of the above categories and is held by a public authority as defined by the FOI Acts (see Schedule 1) or a publicly owned company (Section 5 of the UK FOI Act and section 6 of the Scottish FOI Act). This category divides into two sub-categories: • **Semi-structured data.** This data that is part of, or is intended to be part of a set of information relating to individuals and that is structured by reference to individuals or by criteria relating to individuals but that does not have an internal structure or

	referencing system that would facilitate retrieval of specific information about particular individuals. An example would be a set of case files with a chronological arrangement of papers within each file. • **Unstructured data.** This is data that does not have the type of structure described above. An example would be policy or subject file in which details of an individual occurred randomly.
Public records	Records of, or held in, any department of Her Majesty's Government in the United Kingdom or records of any office, commission or other body or establishment whatsoever under Her Majesty's Government in the United Kingdom, as defined in paragraph 2 of the First Schedule to the Public Records Act 1958. Also records of organisations subsequently included in the table in the above schedule or of those whose records have since been determined as public records by the Public Record Office.
Record	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: 2001).
Record keeping system	An information system which captures, manages and provides access to records through time.
Records management	Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records (BS ISO 15489: 2001).
Record officer	The person appointed by a government department or agency to be responsible for the management of the records of that organisation.
Registration	The act of giving a record a unique identifier on its entry into a record keeping system.
Retention	The continued storage and maintenance of records for as long as they are required by the creating or holding organisation until their disposal, according to their administrative, legal, financial and historical evaluation.
Retention schedule	A means to enable Records Manager to dispose of records promptly, consistent with effective and efficient operations, when the appropriate period of retention has expired.
Review	The examination of records to determine whether they should be destroyed, retained for a further period, transferred to an archival establishment, or presented to a third party.
Semi-current records	Records which are no longer required for the conduct of current business and which are waiting to be appraised for their long term value or disposed of in accordance with disposal schedules.
Survey	An examination of current and semi-current records noting briefly their nature, systems of arrangement, date ranges, quantities, function, physical condition, reference activity and rates of accumulation.

Version control	A process that allows for the precise placing of individual versions of documents within a continuum.
Vital records	Those records that are essential to the operation of the organisation, the continuation and/or resumption of operations following a disaster. The recreation of legal, regulatory or financial status of the organisation, or to the fulfilment of its obligations, in the event of a disaster.

Appendix 2

Relationship with other relevant existing policies, legislation and standards

This policy has been written within the context of the following:

National legislation or strategic or adaptive initiatives

- College of Policing (2014) Authorised Professional Practice: Guidance on MoPI 2010 with online updates
- Criminal Procedures and Investigations Act 1996
- Data Protection Act 2018
- Equality Act 2010
- Freedom of Information Act 2000
- Human Rights Act 1998
- Lord Chancellor's Code of Practice on the Management of Records under S46 of Freedom of Information Act 2000
- Management of Police Information (MoPI) Code of Practice (CoP)
- National Cyber Security Centre 14 principles on cloud security
- National Enabling Programme (NEP)
- National Policing Community Security Policy
- NPCC National Retention Tables 2017/18
- Police Service File Plan (PSFP, 2010, V3.1)
- UK G-Cloud Framework

Local and regional policies and supporting guidance

- Business Continuity Recovery Plan
- Data Protection Policy
- Evidential Property Policy
- Freedom of Information Policy
- Information Asset Owner Policy
- Information Classification and Handling Policy
- Information Management Strategy (IMS)
- Information Sharing Policy
- Information Security Policy
- Quality Assurance and Audit (QA)
- Review, Retention and Disposal Policy (RRD)
- Regional Business and Digital Learning and Development strategies

International or domestic standards and guidance

- MoReq2010® – Model requirements for records systems (European Commission DLM Forum)
- ISO 15489-1:2016 (2nd ed.)(Information and documentation -- Records management -- Part 1: General)
- ISO/TR 21946:2018 Appraisal for managing records
- ISO 16175:2019 Processes and Functional Requirements for software for managing records
- ISO 27001:2005 (Information technology - Security techniques - Code of practice for information security management)
- ISO 22313:2012 Societal security - Business continuity management systems — Guidance
- ISO 23081-1:2006 (Information and documentation -- Records management processes – Metadata for records - Part 1: Principles)
- ISO 15713:2009 - Secure destruction of confidential material
- 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 10008:2014 (Code of practice for legal admissibility and evidential weight of information stored electronically)
- BSI BIP 0010:2004 (The principles of good practice for information management)