Title:	**Records Management**		
Practice / Business Area:	Records Management		
Department Responsible:	Information Management - Systems Maintenance & Security		
First Published:	March 2013		
Last Reviewed:	21/07/2020	This document applies to employees of the:	
Version Number:	09 (external)	Chief Constable	Commissioner

SOUTH WALES POLICE PROCEDURE OBJECTIVE:

Ensure that police services are delivered lawfully and transparently, whilst protecting the integrity of South Wales Police and its staff through effective records management.

PROCEDURE:

Line Management Responsibility:

Information Asset Owners/Chief Officers are responsible for:

- the local BCU development and operation of records management procedures, covering both electronic and hard copy media, that:
  - are efficient / fit for purpose;
  - comply with South Wales Police's records management Guidance and Procedure and standards;
- ensuring that appropriate resources exist within Areas/Departments for fulfilling the responsibilities for managing records;
- communication of Area/Departmental records management procedures;
- quality assurance of Area/Departmental records management processes and procedures;
- ensuring that procedures for the offsite storage of hard copy records are followed.

These responsibilities to Area/Departmental Records Management Teams where these exist.

It is a requirement that any new system or programme to be implemented within South Wales Police **must** have a **Risk Management Accredited Document Set (RMADS)** and **Data Protection Impact Assessment (DPIA)** completed. See the **Force Information Security** and **Data Protection** Guidance and Procedure documents, respectively, on the force intranet for further information on how to complete these documents.

Information Asset Owners:

Information Asset Owners are senior/responsible individuals involved in running their relevant business areas and they are responsible for the processes surrounding the usage of the information and consistency of those processes across the Force. Their role is to understand what information is held; what is added and what is removed; how the information is moved; and who has access and why. As a result they are best able to understand and address risks to the information, and ensure that information is fully used within the law.

It is important to note that the Information Asset Owner role is managing information **not** systems – the responsibility for the functionality, performance and maintenance of each system lies with the respective System Owner. There may, however, be times where the same individual will perform both the Information Asset Owner and System Owner roles simultaneously. They will be able to assist and provide inputs to the Senior Information Risk Owner (SIRO) – a role held by the ACC Specialist Operations - on the security and use of their asset. Information Management hold a collated version of the force's Information Asset Register. An Information Asset Owner Handbook is also provided to Information Asset Owners and Information Asset Administrators – this is available on the Information Management page of the force intranet, under IAO guidance, and Information Asset Owner Training will be provided to all relevant staff.

Cloud Access:

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centres available to many users over the Internet. Large clouds, predominant today, often have functions distributed over multiple locations from central servers. If the connection to the user is relatively close, it may be designated an edge server.

Where cloud storage or cloud based systems are to be utilised, the following applies:

The project lead, introducing the new services (the 'cloud service customer') will be responsible for agreeing with the cloud service provider, an appropriate allocation of information security roles and responsibilities, and confirming that it can fulfil its allocated roles and responsibilities.

The Information Asset Owner (IAO) will define or extend existing policies and procedures to the use of cloud services and make cloud service users aware of their roles and responsibilities in the use of the cloud service.

The cloud provider must clearly document and communicate its information security capabilities, roles and responsibilities for the use of its cloud service.

Any information security roles and responsibilities which the cloud provider requires the IAO and service users to implement and manage as part of its use of the cloud service should also be defined.

Responsibility for project records:

Records relating to projects, which involve two or more Areas are the responsibility of the project manager. Project managers are responsible for:

- identification of project related records and liaison with relevant Areas/Departments to ensure that project records are managed efficiently and comply with South Wales Police's records management Guidance and Procedure;
- ensuring that appropriate resources exist within the project for fulfilling the responsibilities for managing records;
- quality assurance of records management processes and procedures within the project;

- ensuring the appropriate disposition of project records.

Responsibilities of individuals:

Everyone who creates or receives records has a responsibility to follow South Wales Police records management procedures.

Monitoring and auditing:

Where it is relevant to an Internal Audit or Quality Assurance review compliance, with South Wales Police records management procedures, guidance and standards must be included in the review.

Records Management Standards:

View the 'South Wales Police Records Management Standards' on the Information Management pages of the force intranet, under 'Documents'.

Record Creation:

This section provides an overview of the minimum standards required for record collection within South Wales Police (also refer to the 'Public Service Centre Standard Operating Procedures' for further information). These documents outline the defined processes for the departments responsible for record collection within South Wales Police.

The evaluation process will be conducted at the point of input; this will be done in the normal course of work within the existing core systems. It is the responsibility of the systems users and supervisors to ensure that all data entered into the records is to the highest possible quality and meets with the requirements set below:

- ensure information is recorded for a policing purpose;
- ensure information is used to support decision-making through NIM;
- providing an auditable decision-making process;
- provide the ability to evaluate, risk assess and corroborate other related information;
- ensure information is recorded according to the data quality principles – accurate, adequate, relevant and timely *(see also the Data Protection Policy – **DP009 – Data Minimisation, Pseudonymisation and Anonymisation**)*;
- ensure checks are made to avoid creating duplicate records;
- ensure correct Government Security Classification (GSC) protective marking is used (this replaced by the Government Protective Marking Scheme – GPMS and, therefore, some older documentation may be marked using GPMS marking) – for more information refer to the following Information Security Policies:
    - 1.08 Government Security Classification – User Guidance;
    - 2.05 Government Security Classification – Policy;
    - 2.06 Government Security Classification – Security Controls Framework;

- ensure the correct links are made to records within force and to those held within the PNC;
- ensure record creation and management is compliant with the National Crime Recording Standards.

All staff responsible for evaluating information will receive training in the modules of Initial Review and Evaluation as outlined in the National Training and Delivery Strategy for the Management of Police Information with additional workshops and Niche training.

Information from the force's core systems will be copied into the force Data Warehouse. The quality will be checked and searches made for links with existing records (see review processes).

Data Quality:

Good data quality is fundamental to successful information management It is essential that all information is recorded properly **first time, every time**. Failure to get it right at the outset will create additional work, compromise the accuracy and reliability of the information, and ultimately affect the ability of the Force to protect the public. Good quality information helps ensure that the appropriate action is taken and means that the information can be shared with other forces and agencies and used with confidence. Information must be accurate, adequate, relevant, and recorded in agreed timescales.

Refer to the 'Data Quality procedure and guidance' for further information.

Review, Retention and Disposal of Records, including Custody Images and Biometrics:

Documents will be retained for the period specified in the South Wales Police **Record Retention Schedule** (the latest version can be found on the Information Management page on the force intranet, under "Retention Schedule". Previous versions will also be made available for continuity purposes).

The primary purpose of the review, retention and disposal procedures is to protect the public and help manage the risks posed by known offenders and other potentially dangerous people. The review of police information is central to risk-based decision making and public protection. Records must be regularly reviewed to ensure that they remain necessary for a policing purpose, and are adequate and up to date.

South Wales Police has standard procedures in place for reviewing records and making accountable decisions on the retention or disposal of information. Review procedures ensure that information retained by the police service is held lawfully, and may help to prevent forces being overloaded by the volume of information captured and recorded.

Custody image management will be in line with the review schedule for management of police information (MoPI) groups. Images will be considered for deletion at the first scheduled review, including clear periods. The review schedule within the College of Policing's Authorised Professional Practice (APP) on Information Management should be used to manage the process.

However, an individual is able to apply to request deletion of their custody image where they were:

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

Where an individual who was not convicted makes an application for deletion, there should be a presumption in favour of deletion. The Records Deletion Panel, in conjunction with the Senior Information Risk Owner (SIRO – ACC) and Data Protection Officer have the discretion to retain a custody image where this is necessary for a policing purpose and there is an exceptional reason to do so. Examples might include where the individual is considered to pose a substantial risk of harm when assessed against national retention assessment criteria (NRAC).

The process for requesting deletion of custody images forms part of the **DP006 - Records Deletion Process**.

The force **Record Retention Schedule** provides definitive instruction for the retention of **all** records held by South Wales Police, including electronically stored records and physical records. This schedule is maintained by the Information Sharing Agreements and Records Management Officer based on national guidance.

Where it is identified that certain records or documents are not listed within the Retention Schedule, this must be raised with the Records Management Officer in Information Management who will advise on relevant retention periods and will arrange for these to be signed off by the SIRO, via the Information Assurance Board (IAB).

See also the “Public Inquiries” section of this Procedure and Guidance document.

Public Inquiries:

Where a moratorium is placed on the destruction, disposal or alteration of certain records, this will be added to this section and also to the Record Retention Schedule.

S.35 of the Inquiries Act 2005 makes it an offence for a person to alter or destroy a document they know to be relevant to an inquiry.

At the time of publication, there are two Public Inquiries that currently impact on the destruction, disposal or alteration of records:

- *Undercover Policing Inquiry*
  There is a currently a moratorium on the disposal of records relating to undercover operations following a directive from the Inquiry. This Inquiry was formerly known as the ‘Pitchford Inquiry’.

- *Independent Inquiry into Child Sexual Abuse (IICSA)*
  There is a currently a moratorium on the disposal of records relating to child sexual abuse following a directive from the IICSA. This Inquiry was formerly known by other names, including the ‘Goddard Inquiry’.

Interview Tapes and DVDs (Storage and Handling) – Suspects, Victims and Witnesses:

Following the interview, the interviewer will make a note in their manual or electronic pocket notebook to state:

- that the interview has taken place and it was audibly recorded;
- the time it commenced;
- the duration of the interview; and
- the date and identification number of the master recording.

The recording media must be kept and handled securely as set out in the following Codes of Practice for the Police and Criminal Evidence Act 1984 (PACE):

- Pace Code E – Code of Practice on Audio Recording Interviews with Suspects
- Pace Code F – Code of Practice on Visual Recording with Sound of Interviews with Suspects

In respect to the storage, custody and destruction of video-recordings of interviews, please also refer to the Ministry of Justice's "Achieving Best Evidence in Criminal Proceedings" (March 2011) document, which provides guidance on interviewing victims and witnesses, and guidance on using special measures.

For more information on managing Interview DVDs, please refer to:

- Criminal Justice - Interview DVDs page
- Criminal Justice - Interview Transcription page
- Visual Recordings – Making, Storing and Destruction procedure and guidance

Documents will be retained for the period specified in the **Record Retention Schedule**, in line with the relevant MoPI Group on the most serious offence being investigated as part of the interview. See the Review, Retention and Disposal of Records section of this Procedure and Guidance document for further details in respect of the review, retention and disposal of these records in line with MoPI guidelines.

LEGISLATION & REGULATION:

- Freedom of Information Act 2000
- Data Protection Act 2018
- General Data Protection Regulation - Articles
- General Data Protection Regulation - Recitals
- Limitations Act 1980
- Police and Criminal Evidence Act 1984
- Criminal Procedure and Investigations Act 1996