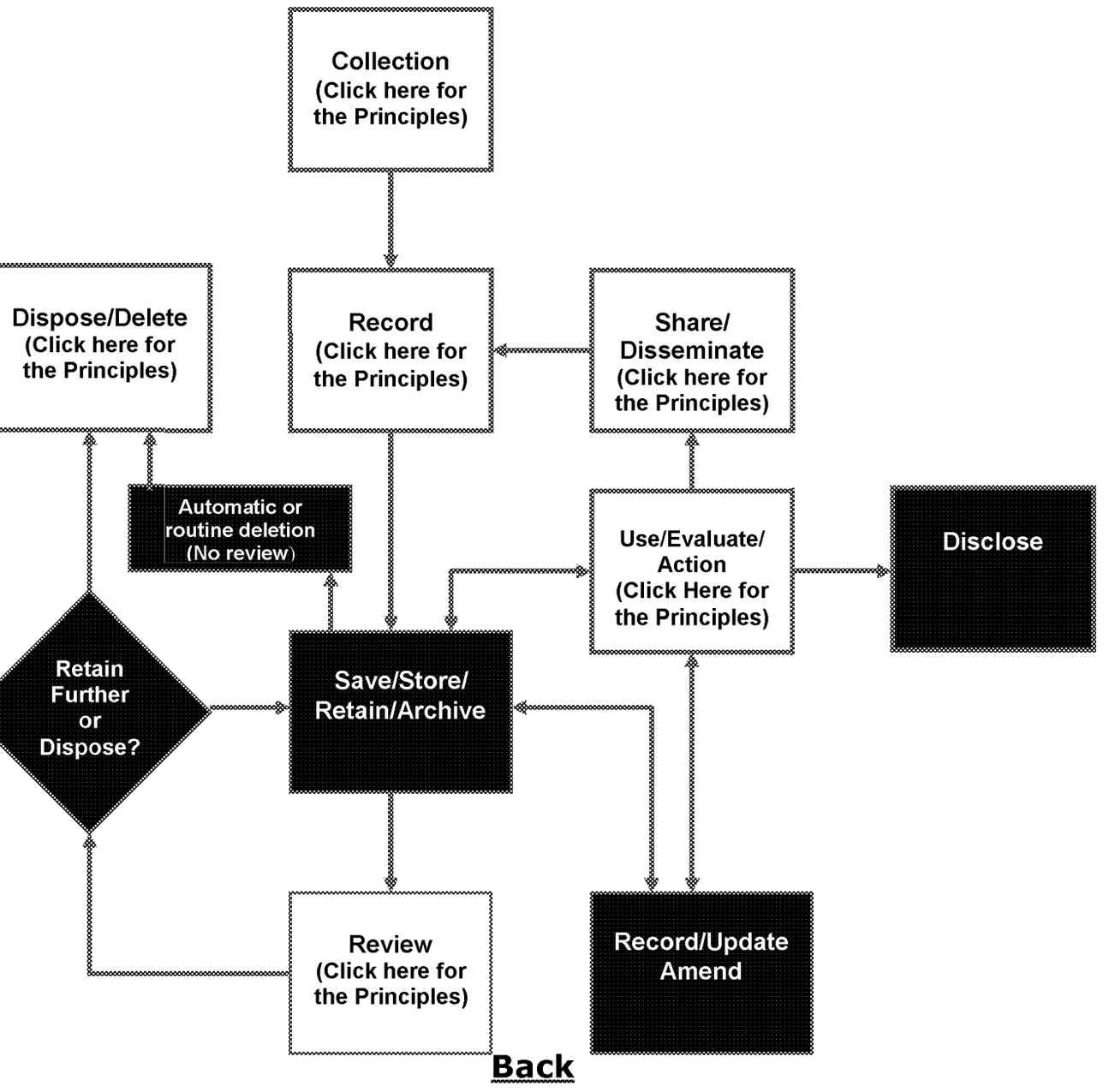
The Information Life Cycle

Navigate to the Handling Activities by Clicking on the Active boxes below



Collecting and Recording

Key = Users | Supervisors | Managers

If your team carries out this task involving information for a Policing Purpose

- Is the information for a policing purpose?
  1. Protect life and property
  2. Preserve order
  3. Prevent the commission of crime
  4. Bringing offenders to justice
  5. Any duty of responsibility from common of statute law
- Are you aware of your local control strategy and priorities which set the intelligence requirements for your department?
- Do you Record the information in the appropriate format and location according to force and local guidance
- Ensure recorded information is relevant, accurate and adequate, meets Force data quality standards and that any personal information meets the data protection principles and duty of confidence requirements
- Ensure that person records are unique by searching before creation and linking information or cross referenced where appropriate

- Provide briefings on the collection of information
- Provide opportunity for debriefing operations
- Ensure your staff follow and keep up to date with changes to Force policies, procedures and guidance.

more

Collecting Key Principles

- Collection is the first stage in the management of police information
- Police information is collected for a policing purpose
- Police information is collected in line with requirements defined by the NIM process
- Information is collected in one of 3 ways – routine collection, tasked information and volunteered information.

References

MoPI Guidance chapter 3

Recording Key Principles

- Police information will be recorded for a policing purpose
- Police information must be recorded correctly first time
- Recorded information should be retrievable and searchable by all those who might need to access it, now or in the future

Back

- **Provide a regular dip sample of records to ensure they comply with data quality and recording principles**
- **Are staff recording in the appropriate format?**
- **Provide staff with feedback for PDR on record creation**
- **Ensure that the recording Checklist is in place and adhered to**
- **Check for timely submission to the organisational memory (Normally by end of shift)**
- **Ensure user of systems are aware of and adhere to relevant procedures for those systems**

- **Ensure that clear intelligence requirements have been set**
- **Ensure that the control strategy drives the intelligence requirement**
- **Ensure staff are aware of what the intelligence requirements are**
- **Ensure data quality is treated as a priority**
- **Ensure there is the ability to link and cross reference information across different business areas**
- **Ensure staff responsible for recording information are trained appropriately**
- **Ensure quality assurance processes exist and are adhered to including; dip samples for compliance with data quality, accuracy, adequacy, relevance and timeliness (AART).**
- **Follow the recording principles (policy /guidance)**

- Police information may be recorded in different business areas depending on its purpose
- Person records held in different business areas should be inter-linked or cross-referenced
- Person Records should meet the requirements of the Data Protection Act 1996 and the common law duty of confidence requirements.

References

MoPI Guidance chapter 4
Force Policy on Recording Information
Force Policy on Data Quality
Force Guidance on Recording Information
Data Protection Guidance
Common Law Duty of Confidence (see http://www.crimereduction.homeoffice.gov.uk/infosharing22-1.htm)

Back

Evaluation and Actioning

Key = Users | Supervisor | Managers

If your team carries out this task involving information for a Policing Purpose

- **Is the information for a policing purpose?**
- **Are you aware of your local control strategy and priorities which set the intelligence requirements for your department?**

- **Provide briefings on the collection of information**
- **Provide opportunity for debriefing operations**
- **Ensure your staff follow and keep up to date with changes to Force policies, procedures and guidance.**

- **Ensure that clear intelligence requirements have been set**
- **Ensure that the control strategy drives the intelligence requirement**
- **Ensure staff are aware of what the intelligence requirements are**

Evaluation and Actioning Key Principles

- Information will be evaluated and risk assessed for its provenance, accuracy, sensitivity and continued relevance
- Information recorded through the 5x5x5 process will undergo evaluation by the relevant intelligence unit
- Evaluation allows for action to be determined and priorities to be identified, proportionate to the nature of the information
- Through evaluation, links with other police information recorded elsewhere are identified
- Evaluation enables the quality assurance of police information

References

MoPI Guidance chapter 5 and Appendix 2
The National Intelligence Model Summary (Guidance)
Force Policy on Intelligence
5x5x5 Intelligence Information Report (Guidance)
Force Guidance on Briefing and Debriefing

Back

Information Sharing and Disclosure

Key = Users | Supervisors | Managers

If your team carries out this task involving information for a Policing Purpose

- **Ensure that the information is relevant, accurate and adequate for the purpose for which it is being shared**
- **When personal information is being shared, the requirements of the Data Protection Act and the common law duty of confidence have been fulfilled**
- **Apply GPMS when sharing personal information or apply a risk assessment where an ISP or statutory purpose to share does not exist.**
- **Information shared should be recorded according to the Force guidance**
- **Ensure the information shared meets a policing purpose and is proportionate and necessary**
- **Ensure information is disseminated as appropriate**

- **Support staff to share information appropriately**
- **Monitor ad hoc decisions to share**
- **Audit decisions to share including necessity, accuracy and adequacy to share**
- **Check if it meets a policing purpose or other legal duty**
- **Ensure information shared does not compromise any police operation or safety to others**

More

Sharing and Disclosure Key Principles

- Policing requires information to be shared within the service, with partner agencies and the public
- Information should not be shared as a matter of routine: each case must be viewed individually with informed decisions made about whether to share or not
- Police forces should actively seek opportunities to share non-personal information. Personal information needs to be shared but is subject of certain safeguards of which all police personnel should be aware.
- The basis for sharing police information is either:
  - Establishing a legal gateway (statutory obligation/statutory power)
  - Identifying a policing purpose for sharing and undertaking a risk assessment (MoPI Checklist 3 provides the details of this risk assessment format)
- Information sharing agreements (ISA) between the police and partner agencies should be used to ensure consistent and proportionate sharing.

Back

- **Ensure a risk assessment is adhered to by the user when making a decision to share**
- **Ensure that ISP's are reviewed in accordance to Force policy**
- **Provide feedback on sharing through the PDR process**
- **Ensure staff follow and keep up to date with changes to Force policies, procedures and guidance**

- **Support staff to manage information appropriately**
- **Ensure staff record decision , in a shared location, on whether to share information or not/ whether information has been shared or not**
- **Ensure all ISP's are held and centrally managed within the Force and reviewed at regular intervals**
- **Ensure that the process of sharing information is adhered to both by those in a user and supervisory capacity**
- **Ensure ISP's are created and authorised through the Force procedure for the development of ISP's**
- **Ensure that staff who have a responsibility for sharing information are trained appropriately**
- **Ensure arrangements in place to conduct dip sampling**
- **Information shared, disseminated or disclosed must be recorded in line with force procedures and system(s)**

References

MoPI Guidance chapter 6
"Working with other Agencies" (Supporting Information)
Force Policy on 'Disclosure of Information' (being updated)
Force Guidance on 'Information Sharing' (to be written)
"Multi-Agency Information Sharing Protocol for Surrey" [The Golden Rules can be found on page 34]

Note: the terms ISP (Information Sharing Protocol); ISA (Information Sharing Agreement); and MOU (Memorandum of Understanding) are all captured by the use of the term ISP).

Data Protection Guidance
Common Law Duty of Confidence (see http://www.crimereduction.homeoffice.gov.uk/infosharing22-1.htm)

Back

Review & Records Disposal

Key = **Users** **Supervisors** **Managers**

Anyone who checks a new or updated record should consider themselves as undertaking an initial review and should ensure Data Quality is correct an that the MoPI Review Group is appropriate. Feed back must be given to the record creator if there are any errors.

If your team carries out this task involving information for a Policing Purpose

- Access, understand and follow force security policies and operating procedures

Yet to be agreed, but these activities are likely to be undertaken by specialist units and trained appropriately.

- Follow force or business area guidance for risk assessing and reviewing records
- Establish and enter the review date for a record at the point of creation
- Follow the NRAC when reviewing records to determine their continued necessity for a policing purpose
- Ensure that where information is to be disposed of, duplicates or other information relating to that person are also disposed of, such that related information is no longer retained elsewhere, other than the Disposal Log. Disposal decisions and activities are likely to be undertaken by specialist roles, and according to force policy and procedures

Review, Retention and Disposal Key Principles

- Records must be regularly reviewed in order to ensure that they remain necessary for a policing purpose, and are adequate and up to date
- The type and amount of information held on an individual must not be excessive and must be proportionate to the risk they pose to the community
- The review of police information is central to risk-based decision making and public protection
- All relevant records must be part of the review in order to ensure a fully considered decision
- The review process should be documented for audit purposes. This will generally be through use of the National Risk Assessment Criteria (NRAC)

Back

Yet to be agreed, but these activities are likely to be undertaken by specialist units and trained appropriately.

- Authorise the outcome of all reviews conducted in their area of responsibility
- Provide feedback to staff on their performance, and through PDR process
- Ensure staff follow, and keep up to date with changes to force policies, procedures and guidance

Yet to be agreed, but these activities are likely to be undertaken by specialist units and trained appropriately.

- Ensure adherence to relevant policies procedures and guidance.
- Ensure that staff responsible for undertaking the reviews are trained appropriately

- Records should be disposed of when there is no longer a policing purpose for retaining them, and a log of the disposal retained for audit purposes. Disposal decisions and activities are likely to be undertaken by specialist roles, and according to force policy and procedures

References
MoPI Guidance chapter 7 and Appendix 4

Back