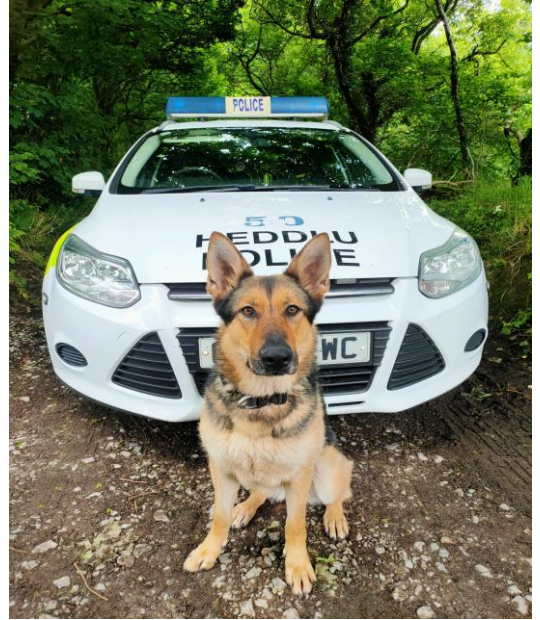




Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Information and Intelligence



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Learners who have successfully completed this lesson will be able to:

1. **Identify** the difference between Information and Intelligence
2. **List** the sources of information available to police
3. **Explain** how NIM applies to a policing context
4. **Describe** how intelligence is graded according to the 3x5x2 System
5. **Demonstrate** an understanding of Managing Information and how this applies to a policing context
6. **Demonstrate** an understanding of the main principles relating to Information sharing

Information

Information is the very life-blood of policing. It may be original & generated by you. It may come from the public or other officers or be fed to you by partner agencies & other sources



Police information is: All the information obtained & recorded for a policing purpose (Source: APP on Information Management)



QTS – what is information?

In your role you will need to identify information from a variety of such sources, both human and technical, and be aware that it has the potential to become intelligence.

Depending on what it is, the information gathered may support both local and national policing objectives and you will need to be able to work in accordance with the requirements of the National Intelligence Model and the principles of managing police information and intelligence.

You will be gathering information, evaluating and conducting an initial assessment of it, grading it, and reporting it in the proper way.

The processes for its review, retention and disposal are unlikely to be something with which you will become intimately involved but they are aspects you need to be aware of.

Information – everyday the police collect information, but it should only be collected if deemed **relevant for a policing purpose**. This provides the police a legal basis to deal with the information, i.e. recording, sharing it with other agencies or simply retaining it for a future use.

Information normally comes from a source that needs no confidentiality, constraints or protection.

It is an overt, i.e. not hidden, piece of information or sequence of communications.

A member of the public calling to report an incident would fit this definition.

All the information obtained must be recorded.

It is essential that all police information is managed lawfully, from its initial collection to its final disposal in order to ensure its lawfulness.

Where might information come from?

Information can be obtained from a wide number of sources.

For the response officer at the front line of policing the first and possibly most readily available source is the community in which that officer works, remembering that community intelligence will usually be based around the perceived problems that the community are experiencing and will need to be processed into usable intelligence.

Information will only be forthcoming if the community has confidence in the police service, force and individual officers. Many times an officer may be told 'I'll tell you but I'm not telling anyone else.'

This will be because that officer may have built up a relationship with that community, is respected by them and is seen as a trusted person.

It is important as an operational officer to understand the value of community intelligence and ensure that gratitude is expressed to the individuals providing it. This will in turn encourage the community to provide intelligence as they will feel that it is being treated seriously, public confidence improves and the cycle continues.

There are many opportunities to gather community intelligence as a community officer but, generally not so many as a response officer who is always on the move from one call to another. The response officer must take every opportunity to use each situation that presents itself to gather intelligence.

For example, information may be gained from someone the officer is interviewing, be it a suspect, the people who know him or a witness or victim.

In most cases when you attend the scene of a crime you will be the Investigating Officer (OIC).

However, on occasions the investigation will be taken over by another officer so it is important that whoever the OIC is they have as much information as possible to help them identify potential witnesses and suspects and thereby solve the crime.

Key source of information is your initial gathering of information at the scene and the crime report you will have completed. If you are aware of the options available to an investigator you will be able to follow, or suggest to others, the areas of investigation that are worth pursuing. The key is information and below are ways of obtaining it.

By and large, the majority of jobs you are given to investigate will start with an instruction from a supervisor or your force's communication centre by radio. It is unlikely that you will be provided with all the information you need to know at the outset, therefore your questioning skills should kick in immediately. If no crimes are revealed, the information regarding the incident will remain just that - information.

Where does information come from ?

External:

- Partner Agencies – e.g. Local Authority, YOTs, Education/ Schools
- House-to-house enquiries

Policy:

- Force Policy / National Guidelines
- CPS Guidelines

Internal:

- Directly/Indirectly obtained information
- CHIS/Test Purchase by undercover officers
- Police intelligence databases
- Police National database (PND)
- I-LEAP
- Social networking sites – such as Facebook, Twitter
- Open sources (search engines)
- Supervisors
- Specialist Department (e.g. NPT/Public Protection)



QTS – where does information come from?

Boardblast answers

Getting hold of as much information at the outset and managing your response accordingly is essential when tasked with a job.

As a matter of course (for your benefit and the good of the investigative process), you will be collecting and recording information in many formats, eg, pocket notebooks, traffic process forms, accident and incident reports, notes for statements etc. These notes highlight how important information and intelligence is to police work at many levels.

The sources of information listed here is by no means exhaustive.

The majority of crime is not witnessed by the police, but in order to solve it they need information from people who have, and this means information must be sought from witnesses. Generally, if there is no forensic evidence, such as fingerprints, information or intelligence that leads the police to a suspect will only be provided by witnesses.

I-LEAP

The I-LEAP programme will provide new alerting digital platform capabilities to police and Border Force officers in the UK, and to their equivalents in partner

countries, enabling increased opportunities at the national border or within country to identify persons and objects of interest to law enforcement agencies.

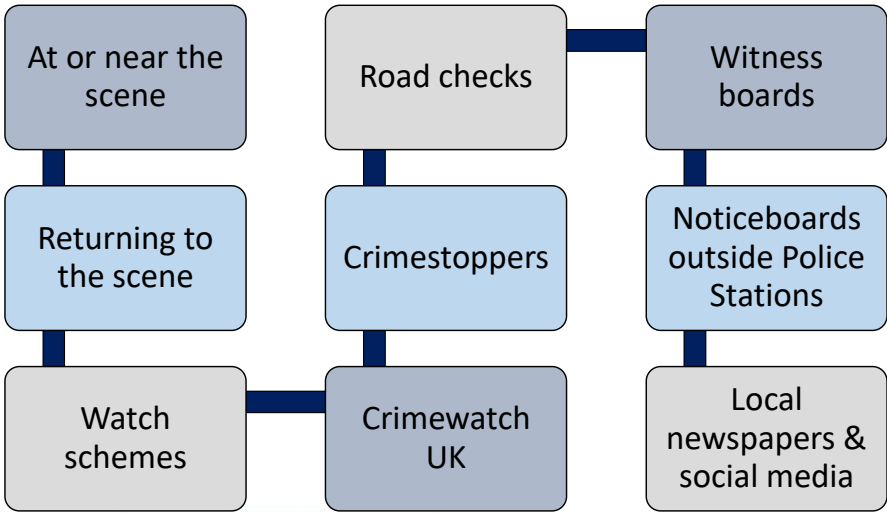
It will do so by first enhancing the UK's connectivity with INTERPOL by providing law enforcement agencies with connectivity to the fixed INTERPOL's network database (FIND) system, providing real-time access to INTERPOL nominal data to UK policing, whilst also expanding access to other INTERPOL datasets. These services are being rolled out nationally to policing, the UK Border Force, and the National Crime Agency (NCA). This is the current priority of the programme.

In the longer-term, the I-LEAP service will expand to provide reciprocal access to international alert data exchange with international partners, initially focussing on a potential multilateral solution with the EU followed by bilateral agreement with other partner countries who share the UK's interest in further strengthening alert-sharing capabilities.

As of December 2022, the I-LEAP capability has been fully adopted across police service Northern Ireland, Surrey, Sussex and counter terrorism policing, alongside new users from Avon and Somerset and Wiltshire police. This represents over 12,000 users across these forces with over half a million searches carried out. Feedback received from frontline police officers has reinforced the importance of real-time connection to INTERPOL circulations, including images, in protecting public safety and tackling criminality.

Information Gathering

There are a number of methods for tracing witnesses including:



QTS – how do we go about tracing witnesses?

Boardblast answers

There are a number of methods for tracing witnesses including:

At or near the scene

Dependent on the type of incident you may need to knock on the doors of houses nearby to enquire if anyone saw or heard anything. These are called house-to-house enquiries, which are particularly important in cases of serious crime where they are tightly controlled by the OIC, who will use a pre-determined questionnaire seeking to ensure that everyone gets asked the same questions.

Returning to the scene

Anyone living nearby may have witnessed the crime, possibly without knowing it, and the only way of finding out if they saw or heard anything of investigative importance is by asking questions to gain information or intelligence. As well as people living nearby, others who were in the general area at the material time could be potential witnesses, eg, postal workers or other delivery people, dog walkers and so forth. By returning to the scene of the crime at the same time the next day, or the same time and day the following week, the OIC might identify people whose daily schedules take them close to the scene.

As the initial or actual investigator you should consider returning to the scene yourself to make further local enquiries. When you do, you should always endorse the crime report with details of what you have done together with any results or future plans.

Local newspapers

Local newspapers serve the community and reporters visit police stations on a regular basis where they are supplied with information about local crimes and other matters of interest, like series of shed burglaries or anti-social behaviour. They are an invaluable contact with the local public and therefore offer an opportunity to appeal for witnesses.

They also run crime prevention articles that provide the public with advice on measures to protect themselves and their property. Usually, there is a department responsible for supplying this press information – Corporate Comms.

Crimewatch UK

This is a regular, nationwide TV programme that appeals for witnesses and owners of stolen property. They televise reconstructions hoping to jog people's memories. It usually focuses on the more serious crimes, but next time it is televised look at the sorts of information the OICs are asking for.

There is a formal procedure which forces follow in order to have a crime included so find out what it is and who is responsible for coordinating it.

Crimestoppers

This is a similar programme on the local radio. The difference is that an informant may earn a reward for information provided. When members of the public contact them they do not talk directly to police officers and there is a public telephone number for them.

Road checks

In the case of serious crimes, an officer of the rank of superintendent (or above) has power under the Police and Criminal Evidence Act to authorise the setting up of a vehicle road check for the purpose of seeking witnesses, suspects and persons at large.

Witness boards

These are free standing signs placed at the scene of a serious road traffic collision or serious crime. They provide brief details of the incident, eg, date, time and nature, together with an appeal for help, along with details of the police station dealing with it so the public can make contact.

Notice boards outside police stations

Some stations have an outside notice board which is clearly visible to members of the public and holds appeals for all sorts of information and witnesses. Have a look at the one outside your station and see what is displayed.

Watch schemes

There will be a number of Neighbourhood Watch (NHW) schemes operating in your area. They each comprise a network of local residents, with a local coordinator, who act as the eyes and ears of the police. They are an important component of the police/public contract in the fight against crime and provide a means for the two-way flow of information between police and public. A word with the local NHW coordinator may produce a result since they can ask around and find witnesses that the police might not.

Since the introduction of the NHW scheme, a number of other schemes have developed to cover specific areas and some of them may operate where you work:

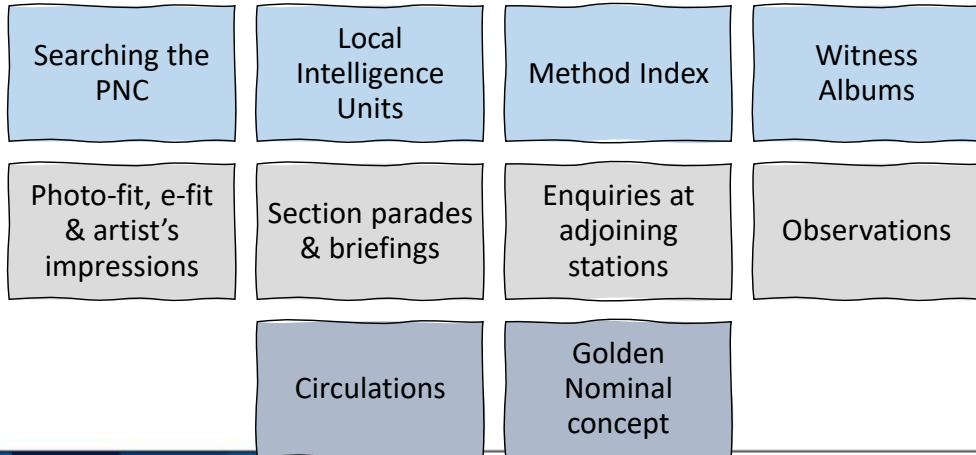
- ☐ Farm or Country Watch - to protect farm property, livestock and machinery
- ☐ Factory Watch - to protect premises on industrial estates and the like
- ☐ Boat Watch - to protect craft and plant moored at marinas and elsewhere
- ☐ Pub and Shop Watch.

There will be someone responsible for the overall coordination of such schemes – normally run and managed through the Neighbourhood Policing Teams.

Not all the methods described above would be used in every crime investigation - it will depend on the circumstances of each case and the decision of the OIC.

Information Gathering

The information gathered from witnesses may provide details leading to the suspect. To help trace that person the Investigating Officer may use some of the following methods:



Searching the Police National Computer (PNC)

The computer is accessible 24 hours a day, 7 days a week, 365 days a year and the principal indices held on it, each of which contain extensive profiles, relate to:

- ☐ People
- ☐ Vehicles
- ☐ Property
- ☐ Information directories
- ☐ Broadcast messages
- ☐ Details of personal characteristics, including specific mannerisms, styles of dress and specialist skills
- ☐ Details of occupations, known associates and police officers who have specific knowledge of the person.

All the information contained in the database originates from officers like you; the amount of information and its accuracy depend on you submitting accurate information on crime reports, arrest reports and intelligence items.

Local intelligence units

In order for the police to be pro-active in the fight against crime, the gathering, evaluation and analysis of information about criminals is essential.

Local Intelligence Units analyse information and intelligence from crime reports,

detention records, intelligence reports, electoral rolls, premises searched records, stop and search records, and many other sources. This enables them to spot patterns and possibly connect crimes to help identify prolific offenders. It is possible that there are details of connected crimes that could assist you or another OIC in solving your particular offence.

Method index

The National Records Office, located at New Scotland Yard, maintains a Method Index which holds searchable records regarding, for example:

- ☐ Unnamed suspects by description and method used
- ☐ Unsolved crimes by method used
- Nicknames including Citizen Band radio call signs.

(Even at the local level, as the investigator it is important for you to consider and report on the method (modus operandi or MO) used in a crime, especially if it was unusual in any way and/or if it was similar to other offences in the area because this might help trace the offender. This in turn might facilitate offences Taken into Consideration (TICs))

Witness albums

Most forces maintain a collection of photographs of convicted criminals (along with their fingerprints). If a witness saw a suspect they can, in certain circumstances, be shown albums of photographs of people who match the description given by the witness. If the witness is able to identify the suspect from a photograph it will provide the investigator with the name and other details of the possible offender.

Photo-fit, e-fit and artist's impressions

Although normally used for serious offences, where a witness is able to provide a detailed description of a suspect from memory, a photo-fit, e-fit picture or an artist's impression can be built up. Such pictures can be used in any appeals to the public for the identity of the person.

Section parades/briefings

A good source of information is your colleagues. At the start of a shift there is normally some form of parade where tasks and information are issued to officers. This may be conducted in person by the sergeant or inspector or by way of computer. Either way, it is an opportunity to ask your colleagues if they have any local knowledge or recent sightings of a suspect.

Enquires at adjoining stations

Criminals don't limit their activity to within walking distance from home so it is possible that crimes with a similar method or having a suspect of similar description may have been committed in areas covered by adjoining stations. Enquiries there may produce useful information and help solve not just your crime but others you may not be aware of.

Observation

If it is known that a suspect frequents or is operating in one particular area, consideration should be given to organising “observations” in order to catch them - watching and waiting often yields results.

Circulations

Where a suspect has been identified and there are reasonable grounds to suspect that that person has committed an offence (such that it would justify an arrest) we can circulate details of the person as “wanted”. There are a number of ways in which such information can be circulated.

□ **Police National Computer (PNC)** PNC holds a database of all persons who are sought for arrest. Each record will contain details of the person wanted, a description, reason wanted and details of the force and station dealing with the case.

Provided full and accurate information has been submitted for inclusion on the PNC, if your suspect is stopped or arrested in any part of the UK, he or she will be flagged up as being wanted by you.

It is important that the wanted notice on PNC is cancelled as soon as your suspect is arrested - if not, they may be arrested again for the same offence, which could amount to an unlawful arrest. It is the IO’s responsibility to do the cancellations.

The Police Gazette and other publications The Police Gazette and other such publications are rather like police newspapers that contain information of interest to officers throughout the UK. Forces submit items they wish to be circulated in such publications; these may relate to wanted persons, persons sought for interview, unidentified bodies, missing persons or unidentified property etc plus cancellations of previous entries.

They are circulated to every police force and copies of them are held at most stations.

Golden Nominal Concept

Golden Nominal is a term used within the Public Sector and concerns the strive towards a single view of citizen information. Police forces and other government agencies have an increasing focus to understand and effectively use the data that is often collected across multiple touch points. **(Experian)**

<https://www.experian.co.uk/blogs/latest-thinking/data-and-innovation/case-study-cleveland-police/>

It showcases how the power of better data positively impacts on policing.

The Police collect huge amounts of data, often in challenging circumstances. The result is a very high number of duplicate and incomplete person records within the

main policing system. The scale of the issue is vast and impossible to quantify. Removing the need to search through duplicate records would provide a holistic view of one person and their interactions. This can better expose any potential threat that they pose to the community or how vulnerable they may be and enable a response that's far quicker and more appropriate to the situation.

Significantly less time would be required to manually link and manage duplicates, saving valuable resources.

Give handout to students

Intelligence

Intelligence is: Collected information that has been developed for action & may also be classified as confidential or sensitive (Source: APP on Intelligence Management)



Basically, this means information that has been formally processed (Collated & analysed) but it does not only relate to crime & criminality. It is NOT necessarily evidence



QTS – what is the difference between information and intelligence?

Intelligence in an investigative context may be considered a form of information but of a 'special' kind. It is information which has taken on a special meaning.

Quite often it is information gathered covertly from a variety of sources (some confidential), which has been processed, i.e. recorded, graded and evaluated. Intelligence is information which has been **processed** to turn it into usable intelligence, then developed for action and policy making. (3x5x2)

This development ensures ethical, accountable and transparent practice is taking place.

Intelligence is information converted into a state where the police may decide to take action to address e.g. a crime/ASB problem

Intelligence is used to build a picture of unlawful activities, to convert the information into evidence, which can be used to prosecute offenders

Information from the witnesses who do not wish to make a statements could be intelligence.

The whole process is known as the **Intelligence Cycle**.

The process can be compared with a potter's wheel - It is a never-ending, circular process. The information is the clay in a very rough untreated form which, with patience and expertise, can be worked into a usable shape and form.

Accurate and timely intelligence gathered, collated and analysed in a professional manner, must be at the centre of law enforcement activity

There are lots of definitions of intelligence. This definition will suffice for our purposes

Before information becomes intelligence it must be processed:

- Establishing its provenance
- Corroboration
- Correlating it with other information and existing intelligence

Once it has been developed it is then used to help formulate action plans and policy to support national and local priorities.

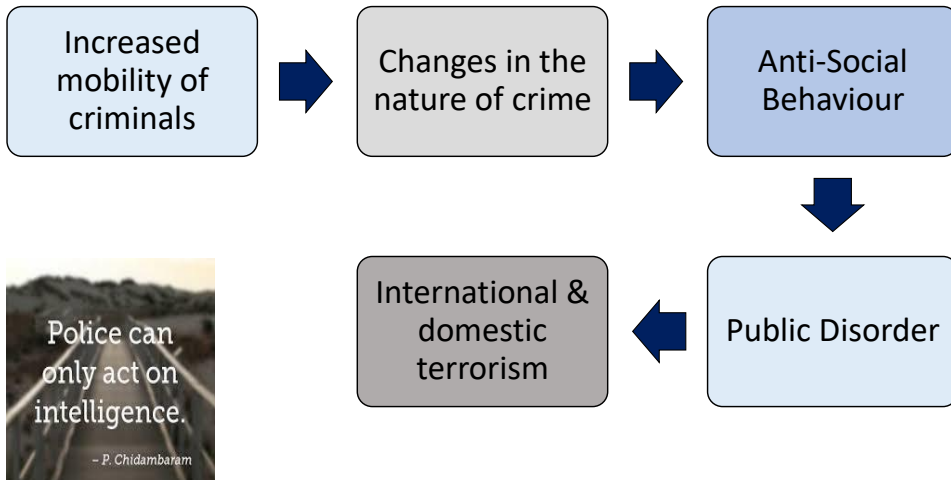
Not all intelligence goes on to become evidence, the majority is used to indicate possible offenders or to predict future events.

The trainer should briefly explain that information can be either 'directly' or 'indirectly' received and provide examples of each.

Because our resources are finite and the call on them is ever increasing it is essential that the available resources are used in the most effective way.

Intelligence allows us to focus on the future by predicting future events.

Why do we need Intelligence?



The need for intelligence does not relate only to crime.
It relates to all areas of operational policing.

Criminals have become far more mobile and no longer commit offences in their own neighbourhood, they travel the length and breadth of the country, overseas, to Europe and other countries further afield. In order to combat this we need to work with other police forces at home and abroad to share intelligence.

The nature of crimes committed has become more sophisticated and hi-tech.

There has been an upsurge in terrorist incidents involving groups from different parts of the world. On the domestic front groups of activists such as Animal Liberation Front (ALF), environmental groups are prepared to use violence and terrorist tactics to further their cause.

Anti-social behaviour has become much more of a problem.

Public disorder at protest marches, demonstrations and sporting events is now more common.

Accurate intelligence may predict possible disorder and crimes, and so resources can be deployed to prevent their occurrence or to arrest offenders.



The trainer should emphasize the rationale/benefits of intelligence led policing

The concept of intelligence led policing is comparatively modern as traditionally we have been demand led, however some recent events have caused the police to be more of a proactive service

In the 1950's with the development of the Motorway network, travelling criminals became a big problem and in an effort to combat this and increasingly organised crime, the first intelligence unit was set up at Scotland Yard, this is known today as SO11. This was such a success in gathering intelligence on crime, criminals and their associates that in 1963 similar units were established in Cardiff, Durham, Liverpool, Glasgow and Manchester

In 1967 building on the success of these intelligence units, Collators were introduced across the country at Divisional level

The Baumber report, 1975, the first National Police Report on intelligence introduced the concept of Regional Intelligence Offices and Force Intelligence Bureau and 3 years later 9 RCIO's were subsequently set up across the country

In 1992 the National Criminal Intelligence Service was formed by combining other national intelligence agencies i.e. National Football Intelligence Unit, Extortion Unit etc.

National Intelligence Model 1999 - discussed later

The National Intelligence Model (NIM)



Standardised framework to place intelligence at the forefront in reducing crime & disorder



Informs strategic & tactical decision making



The National Police Chief's Council (NPCC) has signed up to NIM and all 43 police forces within England, Wales and Northern Ireland are now implementing the Model to commonly accepted standards and 'arrangements for implementation should be set out in local policing plans'.

Launched by NCIS, and adopted by the Association of Chief Police Officers (now the NPCC) in 2000, the government placed the NIM at the centre of the Police Reform Agenda.

The National Intelligence Model (NIM) is a 'Model for Policing' that ensures information is fully researched, developed and analysed to provide intelligence to senior managers to:-

- Provide strategic direction.
- Make tactical resourcing decisions about operational policing, and
- Manage risk.

It aims to ensure that policing is delivered in a targeted manner through the development of information and intelligence. NIM is applicable to all aspects of operational policing because it enables managers to prioritise activities and resources.

It is important to note that the NIM is NOT just about crime and NOT just about intelligence - it is a model that can be used for most areas of policing.

The **National Intelligence Model** brings all the best practices in intelligence-led policing together, offering a blueprint for those who wish to develop better their ability to answer critical questions about strategy and tactics

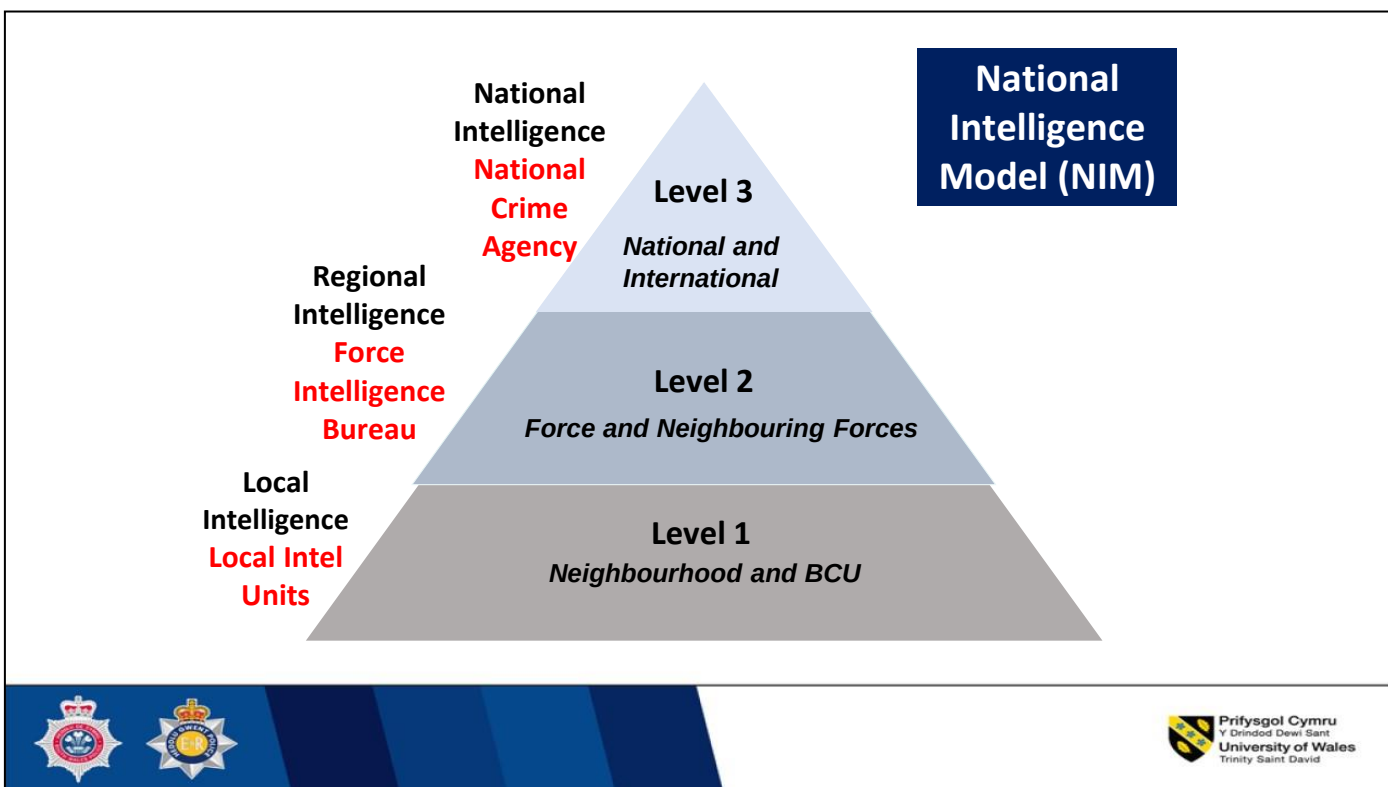
NIM is:

- concerned with using intelligence to determine priorities for policing.
- It is a model for policing that senior managers can use to help them to determine the strategic direction and make tactical decisions about resourcing and operational policing to support local and national objectives
- it also helps manage risk.

Therefore, **NIM** is not just about intelligence gathering, it is also **a business process** model that can be used to guide all activities of a police force.

Advantages of NIM:

- allows operational strategies to focus on key priorities
- allows more officers to focus on solving priority problems and targeting the most prolific and active offenders
- informs the management of risk
- provides more informed business planning and a greater link to operational policing issues
- improves the direction and briefing of patrols
- improves integration with partner agencies



The model works at three levels:

Level 1 - deals with crime, incidents & neighbourhood priorities occurring at a local Basic Command Unit (BCU) level. **Local Intelligence Units** provide intelligence to operational officers within BCUs or areas & will vary in staffing levels. The intelligence you submit as an operational officer will be submitted via Local Intelligence Units.

Level 2 - deals with issues affecting a group of BCUs, neighbouring forces or a group of forces. **FIB** is the **Force Intelligence Bureau**, who deal with serious & inter-force intelligence. Within this department are specialists such as interception of communication experts etc.

Level 3 - is dealt with by the National Crime Agency (NCA) & UK Border Agency which operate on a national or international scale. The **National Crime Agency** handles serious and organised crime as it affects the UK. It is divided between seven regional offices. As well as developing strategic pictures of the different areas in which organised crime operates, the UK Division also collates and analyses intelligence on the UK's top criminal groups & their key players. NCA is also a one-stop shop for UK law enforcement's international enquiries.

First:

1. Certain key 'Assets' must be in place at each level to enable intelligence to be

produced. Without them, the intelligence function will not operate efficiently.

2. A sufficiently flexible 'Tactical Capability' must also be present at each level to deal with identified problems. Without it, too much intelligence will be produced with little or no capability to deal with it. **(Give Hand out: Impact Assessment and Information Asset Owner for further reading)**

Second:

Four key 'Intelligence Products' are produced to drive policing through the Tasking and Co-ordinating process:

The Strategic Assessment - The aim of the Strategic Assessment is to identify the medium to long term issues that are apparent or emerging & to determine resource, funding & communication requirements. A further aim is to ensure there are links covering Level 1, 2 & 3 criminal activities between local, regional & national agencies. While BCUs & forces will produce strategic assessments covering Level 1 & Level 2 issues, & in certain police areas the production of a Level 3 strategic assessment, the UK Level 3 threat assessment shall be the responsibility of the National Criminal Intelligence Service

The Tactical Assessment - The aim of the Tactical Assessment is to identify the short-term issues which require attention & to monitor progress on current business in line with the control strategy. The areas the Tactical Assessment will cover will include appropriate interventions for intelligence gathering, enforcement & prevention activities; the identification of emerging patterns of crime & incidents; & a performance assessment

The Problem Profile - The purpose of a problem profile is to provide an assessment of a specific problem or series of problems which may be criminal, which may pose a threat to public safety or may be anti-social in context. The profile will include an analysis of the problem with recommendations for intelligence gathering, enforcement or prevention. Problem profiles are ideally suited for existing problem-oriented policing methodologies.

The Subject Profile - A subject profile is a detailed analysis of

an individual or network & should contain sufficient detail to enable a targeted operation or intervention against that person or network. It will also recommend operational intelligence requirements in order to secure the information required to implement a tactical response.

Third:

The Tasking & Co-ordinating Process takes place strategically & tactically at each level with information & intelligence flowing between levels & between neighbouring police forces & law enforcement agencies.

At a strategic level, the NIM is strongly linked to all aspects of business planning, both in relation to the Policing Plans & the strategies of Crime & Disorder Reduction Partnerships.

The description of these levels should not suggest that criminals operate at only three levels. Many criminals operate within all of them, disrupting their local communities whilst operating across local borders.

Why three levels?

Any crime, incident or neighbourhood priority that is evident at the local level (i.e. Level 1) could originate from, or hold implications for, other levels. A key component of the NIM is ensuring that communication & information flows between all three levels in order to maximise the effectiveness & efficiency of any formulated response, whatever the level.

The police collect information that is required for policing purposes. Policing purposes provide the legal basis for the collection, recording, evaluation, sharing & retention of information & may include one, or a combination, of the following:

protecting life & property
preserving order
preventing the commission of offences
bringing offenders to justice
any duty or responsibility arising from common or statute law.

Information is collected in one of three ways:

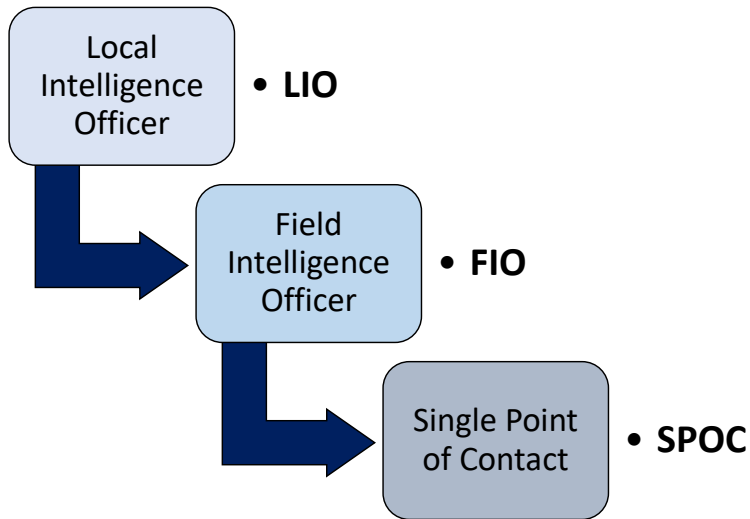
[routine collection](#) – Targeted patrols; stop search; stop & account; responding to incidents

[tasked information](#) – collection of CCTV; CHIS – Covert Human Intelligence Source; ANPR

[volunteered information](#) – a member of the public telling you something, someone from a partnership informing you

Staff should consider the type of information that may be available & the likelihood of it having value as intelligence, based on the [intelligence requirement](#). Collection should be managed by using intelligence collection plans to ensure that it remains focused. This should not prevent staff from submitting information for a policing purpose that is not contained in a current intelligence requirement.

Management of Information/intelligence



There are a number of personnel who are involved in the management of information/intelligence.

These include:

SPOC - Single Point Of Contact - e.g. specified person, usually in FIB (Force Intelligence Bureau), who liaises with the telecommunication industry for the purpose of gathering intelligence. Individual officers must not contact telephone companies direct.

FIO - Field Intelligence Officer - actively seeks intelligence from a variety of sources in support of the intelligence function

LIO - Local Intelligence Officer - manages/processes/collates local intelligence

N.I.M.

If we get it right, it will provide focus to operational policing

It is dependent on a clear framework of analysis of information & intelligence, allowing a problem solving approach to law enforcement & crime prevention techniques



National Intelligence Model (NIM)

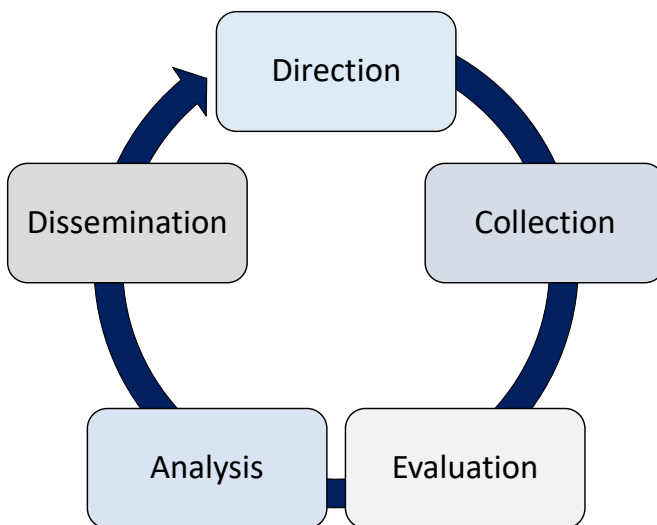
The National Intelligence Model is a method of working based on the principles of problem-solving policing and the use of community and criminal intelligence.

Intelligence Led Policing

Collection, mapping and analysis of Intelligence to aid the efficient management and coordination of police resources.

Basically its about using intelligence to direct patrols to target offending areas (HOTSPOTS).

The Intelligence Cycle



This cycle is a formal model that is a sequential process that allows information to be developed into intelligence, particularly during the analysis phase. By and large, your contributions will come in the collection phase even though they may not have been specifically “directed”.

Processing of information is required to turn it into usable intelligence. This development ensures ethical, accountable and transparent practice is taking place. It is known as the **Intelligence Cycle**. The process can be compared with a potter’s wheel. It is a never- ending, circular process and the information is the clay in a very rough untreated form which, with patience and expertise, can be worked into something with shape and form which can be used.

At the very start of the intelligence cycle is **Direction**

It is essential to have a focused collection plan based on force and local intelligence requirements. These collection plans will be set by the **Tasking and Co-ordination Group Meeting** which is part of the NIM which will be explained later.

The **collection** of intelligence must be done with due regard to legislation such as **ECHR** i.e. legality, proportionality, necessity etc

Standard grounds must be established i.e. likely to be of value in the interests of Prevention or detection of crime and disorder or the maintenance of community safety



Trainer holds board blast on potential collection sources: To include the public, Partner Agencies, internal & external databases:

Sources of information and intelligence, including:

Open/closed sources

Internet Intelligence Investigations (III)

Police National Computer (PNC)

Police National Database (PND)

Policing registers

Other forces/agencies, including specialist agencies and departments

Covert Human Intelligence Sources (CHIS)

Social media

Community intelligence

Digital sources e.g. mobile phones, tablets, laptops, CCTV etc.

The best person to evaluate a piece of information is the person submitting it - **YOU!**

Evaluation is known as the 3 x 5 x 2 system. This system is National and in accordance with the National Intelligence Model. This evaluation process will be covered in more depth later in the lesson

Analysis is carried out to make the best possible use of known information and to produce where possible a predictive element, capable of influencing strategies designed to combat operational problems.

Skilled analysts will then be able to piece together the big picture and develop inferences that will influence operational action. It is at this stage that gaps in intelligence are identified and new targets are identified.

Dissemination - This part of the Intelligence Cycle can only be dealt with after all the other parts have been worked through. This is the point where the Intelligence Specialist decides precisely what to do with the information/intelligence which has been processed.

Dissemination is the passing on of intelligence to those that both should and need to know. Some dissemination requires certain authorities and will be looked at later in the lesson

We can now see the circle is complete, but remember each cycle always must start with a clear direction so we are all pulling in the same direction. Circumstances will invariably change and the process will begin again hence it is a cycle.

Hand Out: Golden Nominal

By getting this right, we can utilise the NIM to create action plans and operations on Strategic and tactical assessments when dealing with incidents of high or low level origins e.g. ASB in local area to Organised Criminal Gangs cuckooing in the area.

The role of briefings is highly important, as it will give an indication of what officer is to do what task within the operation e.g. in a house raid: who is the method of entry officer; do we know the subject/s; are they armed? Who will be the exhibiting officer? Who will be the officer in the case.

What intelligence have we sourced – what does it tell us?

Debriefing the operation is highly important – what have we learnt from it, were there any mistakes made, what went well, what further intelligence did we obtain.

Reporting member of staff and date/time of report

These fields record the name, rank or position, and the station or office of the person who completes the Intelligence Report, together with the date and time of submission.

Or if the report needs to be re-submitted e.g. through sanitisation process, must leave an audit trail.

Relevant Legislation



CPIA 1996
DPA 2018/GDPR (EU)
2016/679 (GDPR)
HRA 1998
FoIA 2000
RIPA 2000
IPA 2016



To be effective the NIM relies on information and/or intelligence which can be obtained from a variety of sources.

There are a number of both legislation, policy and procedures that govern the use of information and intelligence by the police.

What you see here is a list of the legislation, national policies, codes of practice and guidelines that relate to the gathering and submitting of information.

The Criminal Procedure and Investigations Act 1996 provides legislation which lays down provisions for prosecution and defence disclosure to be conducted in stages within criminal proceedings. Duty to record, Retain, reveal (3Rs) and disclosure.

Data Protection Act 2018: protection of information held on databases. Also makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information that should **not be released to anyone not entitled to see it**.

GDPR 2016 (EU) 2016/679 – this is added onto the guidance under the DPA 2018 to form two parts of legislation; GDPR is a lot more sensitive in nature when it comes to holding personal data on individuals e.g. sexual lifestyle/orientation, political allegiance and so on; thus making it in need of more scrutiny and security. As such, sharing of information must fall under some form of governance by the organisation holding the information. This will also fall under the scrutiny of the Information Commissioner Office, who oversee how data is collated, stored and disseminated.

Human Rights Act 1998: protection of life & right to privacy

Freedom of Information Act 2000 also makes provision for the disclosure of information held by public authorities or by persons providing services for them and to amend the Data Protection Act 1998 and the Public Records Act 1958

Regulation of Investigatory Powers Act 2000 mainly deals with the interception of communications, acquiring and disclosing information, carrying out surveillance, the use of Covert Human Intelligence Sources (**CHIS**) and how electronic data protected by encryption or passwords may be decrypted or accessed; it establishes a tribunal with jurisdiction in relation to those matters.

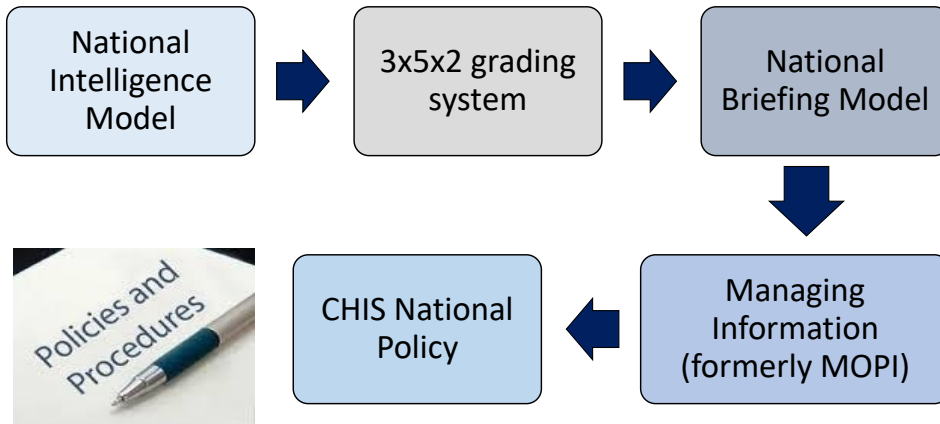
Investigatory Powers Act 2016 (there is a College Learn package on this that students must complete)

An Act to make provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security; to amend sections 3 and 5 of the Intelligence Services Act 1994; and for connected purposes

The act does 3 things:

1. Brings together all of the powers already available to law enforcement and the security and intelligence agencies to obtain communications and data about communications. It will make these powers and the safeguards that apply to them clear and understandable.
2. Radically overhauls the way these powers are authorised and overseen. It introduces a 'double-lock' for interception warrants, so that, following Secretary of State authorisation, these (and other warrants) cannot come into force until they have been approved by a judge. And it creates a powerful new Investigatory Powers Commissioner to oversee how these powers are used.
3. Ensures powers are fit for the digital age. It makes provision for the retention of internet connection records for law enforcement to identify the communications service to which a device has connected. This will restore capabilities that have been lost as a result of changes in the way people communicate.

Policies and Procedures



With regard to policies and procedures we have the **National Intelligence Model** and the **3X5X2 grading system** which will be looking at shortly.

National Briefing Model, is generally more for supervisors although if you were to organise any sort of operation you would use the format outlined in the model.

Managing Information (formerly Management of Police Information MOPI) - 2006

Managing Information relates to the means by which the police collect, record, share and retain information and has been the subject of some controversy in recent years, most notably following an enquiry into the circumstances preceding the Soham murders and the subsequent police investigations (Bichard 2004)

Guidance on the Managing of Information was published in 2006 and sets out basic principles that police organisations should adopt for the collection, recording, sharing and retaining of information relevant to their usual work.

At the level of the individual police officer, this information may take the form of intelligence and evidence gathering, completion of forms and pocket notebook entries. NPCC has published '*Guidance on the Managing of Information*' which is available online

CHIS National Policy

This provides guidelines to Police forces in respect of the use of CHIS.



A source is a person who has access to hidden criminal intentions or plans, and enters into arrangements to reveal this information.

A CHIS will be allocated a 'handler' who will meet them to obtain the information provided as and when necessary.

The operation/handling of a CHIS is strictly controlled under RIPA

How we grade Intelligence when submitting on NICHE

High

- **THREAT TO LIFE, SERIOUS HARM, IMMINENT RISK or OPPORTUNITY** to a child, adult or property

Medium

- **TIME CRITICAL**

Low

- All other criminal intelligence



When submitting intelligence on NICHE officers will initially grade it as red, amber or green dependant on the above criteria.

Trainer to explain that this will be covered in more detail on your NICHE course.

Police Operations



So what's the difference between information, intelligence and evidence in an operational policing context?

Consider a Missing Person enquiry – a teenager has gone missing...

Shannon Matthews Missing February 2008

The police will gather information on the person's usual movements – they may search their room, look at an recent letters, emails, diaries and take their mobile number. **This is just information at this time..**

19th Feb – Last seen outside Westmoor Junior School

20th Feb – Missing Person enquiry and search begun by Police, mothers makes a plea for her return

21st Feb – 200 volunteers join Police to search for Shannon

22nd Feb – Note found in Shannon's bedroom saying she wanted to run away from home

26th Feb – Specialists units assist with the search

1st March - £20,000 reward offered for information

4th March – DNA sample of Shannon taken

5th March – 999 call released to press

12th March – Reward increased to £50,000

14th March – Shannon found alive and hidden in base of divan bed in her Uncles house. He is arrested

8th April – Mother arrested for child neglect, perverting course of justice

- Shannon went missing – **Information? Yes**
- Police spoke to her friend who said that Shannon wants to run away from home and spend more time with her real father. **Information? Yes. Evidence? Not really yet. Intelligence? YES.**
- Shannon is found and she states that her mother took her to her uncles house and locked her in a bedroom and forced her to hide inside a bed. She was not fed for days and was beaten by her uncle. **Information? Yes, Intelligence? Yes Evidence? YES.**

Information - retained, recorded or processed by the police service:

Intelligence – Information which is converted into a state where the police may decide to take action to address

Evidence – Any material that can be used in court eg: testimony made by victim/witness, material objects/exhibits, (real or documentary in its original form, and produced with continuity)

So – information that becomes intelligence becomes evidence – there are no hard and fast rules and there may be some interchange between the different concepts – but generally, the police role is to develop information into intelligence or evidence, depending on the circumstances or the value of the original information (remember the 5x5x5 system).

So – these are different sources of information, but they must all be managed and stored correctly under MOPI and only shared where appropriate.

Remember all these are connected – **CPIA** applies to material gathered in an investigation of a crime – whereas MOPI is about data storage, the DPA is about data-sharing and the Computer Misuse Act is about illegally accessing/using data...



In order to be of use, intelligence must be properly evaluated and its provenance assessed.

The emphasis **MUST** be on integrity in the use of intelligence.

Evaluation of 'raw information' is known as the **3 x 5 x 2 System**

There are three different methods commonly associated with the collection of information.

The information can be collected from a variety of sources – officers, investigations, community, social media, crime stoppers, surveillance, CCTV, Registered sources, or computer data...

You need to be aware that sometimes the source of the information may need to be treated in a confidential or sensitive manner.

The 3X5X2 Intelligence System is simply how the information is recorded on intelligence logs, how it is graded and how it should be disseminated...

This is recorded on a 3X5X2 Intelligence Form (mostly electronic today)...

Evaluations

In order to be of use, intelligence must be properly evaluated & its provenance assessed. The emphasis **MUST** be on integrity in the use of intelligence



Evaluation of 'raw information' is known as the

3 x 5 x 2 system



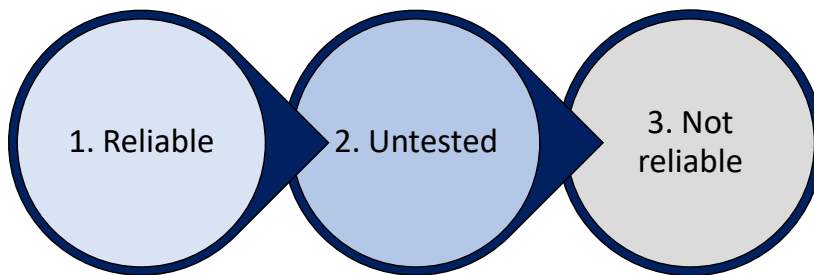
There is a need to separately evaluate both the source and content of each piece of information

This grading affects the sharing, retaining and actioning of the intelligence.

This method establishes the **reliability** and **accuracy** of intelligence and identifies who it should be **disseminated** to.

Source Evaluation

The possible grading's for this part of the assessment are:



The first stage of the evaluation process is evaluation of the source of the information.

Trainer introduces grade 1-3

Explain the importance of establishing provenance of information and its impact on the quality of the information.

How reliable is the source???

1. Reliable - This grading is used when there is no doubt of the authenticity, trustworthiness and competence of the source, or the information has been supplied by an individual who, in the past, has generally proved to be reliable. Examples might include human intelligence, technical, scientific and forensic sources and information known directly to a police officer whose information in the past has always been 100% accurate. Outside agencies & healthcare are also considered reliable given their profession

2. Untested – This relates to a source that has not previously provided information to the person receiving it, or has provided information previously that could not be substantiated. This does not necessarily mean that the information is unreliable but should nonetheless be treated with caution. Before acting upon this information, corroboration should be sought. Examples would apply to information where the

source cannot be determined, i.e. Crimestoppers.

3. Not Reliable – Sources where information in the past, in the majority of instances, has proved unreliable. This evaluation may also be assigned to the information from a technical source where the quality of recording is poor. Other examples might include individuals who have routinely proven unreliable in the past, or there is some doubt about the authenticity, trustworthiness, competency or motive.

Remember, even though this grading system allows the police to make an informed choice about how reliable the source is, they should not accept the information at face value and should **always** seek corroboration where possible.

Intelligence Assessment

There is a need to accurately evaluate the **reliability** of each piece of information:

A. Known directly to the source

B. Known indirectly to the source but corroborated

C. Known indirectly to the source

D. Not known

E. Suspected to be false



Information from intelligence sources will be subject to *evaluation of reliability* before being recorded in the intelligence system

Evaluation must **not** be influenced by personal feelings

Must be based on professional judgement

Its value must **not** be exaggerated in order to ensure action is taken

Officers recording intelligence reports are personally responsible for ensuring the accuracy and proper evaluation of the material based on their knowledge of the circumstances prevailing at the time

There may be occasions when actions launched on the basis of intelligence will have to be defended

****Trainer to emphasise the point that at no time can we task a source to find out any further information – we cannot say to *Mrs Jones* to watch out for the car again and record the VRM or take a description of who is driving etc. To do this we must obtain authorisation from a Superintendent under RIPA / CHIS which we will cover in a few weeks' time. Just be aware that we cannot just do this.**

Information content

The information content should comply with the basic principles of 5WH, ie, what, when, where, why, who and how.

Information should be for a policing purpose. It should be clear, concise and without

abbreviations. The information must be of value and understood without the need to refer to other information sources.

The body of the report should give no indication of the nature of the source, whether human or technical, or the proximity of the source to the information.

Where possible, the information should be corroborated and its provenance established. This could be done through interrogation of information already held in other business areas, for example, PNC. Where research has been done this should be recorded and contained within the initial Intelligence Report (IR) and clearly labelled. It should indicate the databases that have been researched.

For ongoing operations, the operational name or number may be added. A separate IR must be submitted when new intelligence is identified from any research, eg, that carried out on non-law enforcement agency databases (including the internet).

The evaluation of data validity refers to an assessment of the circumstances in which the data was collected, which helps us to understand how “true” or accurate it may be.

- A. Known directly to the source** - Refers to information obtained first-hand, e.g. witnessing it. Care must be taken to differentiate between what a source witnessed themselves and what they were told/heard from a third party.
- B. Known indirectly to the source but corroborated** - Refers to information that the source has not witnessed themselves, but can be verified by separate information that carries the intelligence assessment of ‘A’. Care must be taken to ensure the corroborating information is independent from the original source.
- C. Known indirectly to the source** - Refers to information that has been told to the source by someone else. The source doesn’t have first-hand knowledge of the information as they did not witness it themselves.
- D. Not known** - Refers to when there is no means of assessing the information, such as from an anonymous source i.e. Crimestoppers, this grade should only be used when it is not known how the source knows the information.
- E. Suspected to be false** - Regardless of how the source came upon the information, there is a reason to believe the information is false, when this is the case the rationale for why it’s believed to be false should be recorded in the risk assessment.

Information from intelligence sources will be subject to evaluation of reliability before being recorded into the intelligence system. Evaluation must not be influenced by personal feelings but be based on professional judgement. Its value must not be exaggerated in order to ensure action is taken. It should be remembered that intelligence logs may be produced at criminal or civil hearings.

Handling Codes

The '**Handling code**' provides a risk assessment before deciding to disseminate the intelligence

The handling codes are based on the knowledge of the circumstances at the time by the **person recording the information**.

The two handling codes which can be selected from the drop-down menu are:

P. Lawful sharing permitted

C. Lawful sharing permitted with conditions



The 'Handling Code' is a system that allows officers to record easily their decisions on the suitability or otherwise of exposing the intelligence to other agencies

P. Lawful sharing permitted - Most intelligence will fall into this category, which means the intelligence may be shared with others under the appropriate GSC marking provided there is a policing purpose, local protocols in place and a legitimate need to receive it. If there are concerns of how the intelligence is disseminated, code C applies.

C. Lawful sharing permitted with conditions - This code is used when concerns regarding how widely intelligence should be shared, and that specific handling instructions are to apply. These concerns must be documented within the IR Risk assessment. Action and sanitisation codes must be used.

The intelligence unit will review and may change the handling condition based upon information available to them.

Handling codes are a control mechanism for intelligence sharing. The risks associated with sharing intelligence must always be weighed against the potentially greater risk of not sharing. Handling codes are supported by conditions for intelligence sharing.

Before disseminating intelligence, the person disseminating should ensure they are familiar with the appropriate legislation and their organisation's policies, standard operating procedures and other frameworks.

Lawful sharing permitted (P)

In order to share this intelligence there must be:

- a policing purpose
- local protocols in place
- a legitimate need to receive it.

Lawful policing purpose is defined as to:

- assist others to protect life or property
- assist to preserve order
- prevent the commission of offences
- assist others to bring offenders to justice
- linked to any duty or responsibility arising from common or statute law.

Lawful sharing includes other government departments, private and voluntary sectors.

Specific questions need to be asked when considering dissemination of code P intelligence. For example:

- are there legal obligations?
- who is asking for it?
- why do they want it?
- what are they going to do with it?

Dissemination to European Economic Area (EEA) law enforcement agencies is permitted without any additional IR risk assessment.

If there are concerns around how widely the intelligence may be disseminated, code C applies. It may not be appropriate to disseminate all of the intelligence and the merits of redaction should be considered.

Dissemination to (non-EEA) foreign law enforcement agencies should be risk assessed on an individual basis. The Data Protection Act 1998 allows for personal information to be disseminated outside the EU only after the risks have been assessed and on the grounds of substantial public interest. Public interest in this context includes tackling serious crime and the maintenance of the security and integrity of law enforcement agencies.

Care should be taken when handling intelligence received from HMRC as further unauthorised dissemination may result in the commission of a criminal offence. If this is likely to happen, HMRC will provide a warning within the intelligence report.

Lawful sharing permitted with conditions (C)

This code permits dissemination but requires the receiving agency to observe conditions as specified. Application of this code means the originator has applied

specific handling instructions in respect of this information. An IR risk assessment may be required in respect of the intelligence concerned. An application for public interest immunity should be considered if the intelligence is subsequently used in court.

Handling conditions should be contained within the appropriate section of the IR.

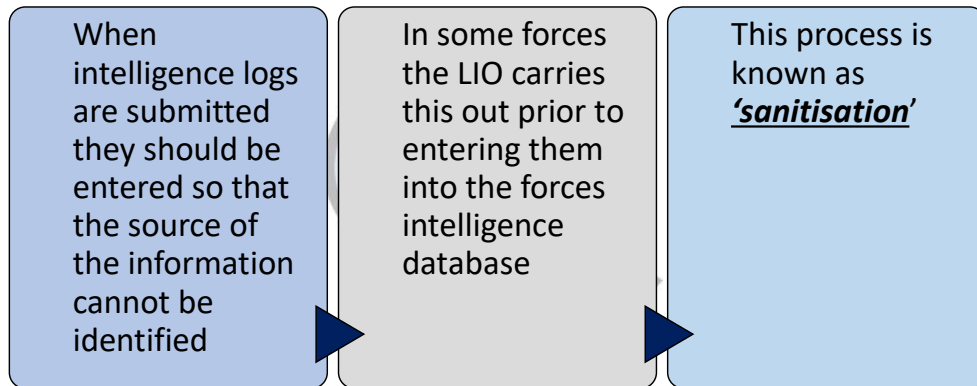
The recipient must abide by the handling conditions. The originator must be contacted by the recipient before they conduct any further activities outside the conditions.

Any intelligence report with conditions should remain under review to ensure that wider dissemination can occur as soon as is feasible, such as when an operation has been concluded or is no longer being pursued.

Conditions – intelligence unit only

- **A1 covert development** – intelligence may be combined or corroborated with other intelligence but action cannot be taken directly. Permission must be sought from the originator before action is taken on any derived intelligence.
- **A2 covert use** – covert action may be taken on this intelligence although the source, technique and any wider investigative effectiveness must be protected. This intelligence may not be used in isolation as evidence, in judicial proceedings or to support arrest.
- **A3 overt use** – overt action is permitted on this intelligence. This information can be used for: TO BE SPECIFIED BY SOURCE INTELLIGENCE OWNER.
- **S1 delegated authority** – the originator of the intelligence permits the unsupervised sanitisation of the material in order to allow dissemination to a wider audience.
- **S2 consult originator** – the originator of the intelligence does not permit the sanitisation of the material for wider dissemination without consultation being sought

Intelligence



Once information has been recorded on a 3x5x2 in an 'unsanitised format', the report should be submitted to the local or force intelligence unit by secure means. It will then be considered for its intelligence value against the BCU or force control strategy, intelligence requirement or other policing purpose.

When intelligence logs are submitted they should be entered so that the source of the information cannot be identified.

In some forces the LIO carries out this prior to entering them into the forces intelligence database.

This process is known as **'sanitisation'**

An LIO conducts the sanitisation of information - occurs when material is removed which explicitly or implicitly identifies a source or an address which is sensitive.



Sanitisation

In some circumstances it may be advantageous to reveal a source's true identity within the body of intelligence without revealing their identity as the source



Where an officer is concerned that the contents of a report might indicate the source, reference should be made to a supervisor before dissemination or entry onto the intelligence system takes place

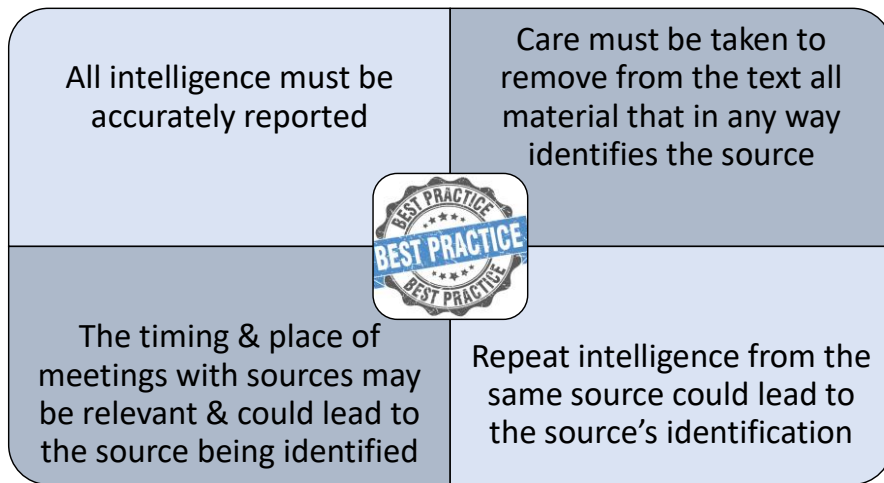


QTS – what is sanitisation?

Sanitisation of information occurs when material is removed which explicitly or implicitly identifies a source. It also occurs when identifying details of a data subject are removed. This process will be undertaken by the intelligence unit prior to the dissemination or inputting onto an intelligence system. Officers / Staff can help this process, however, by understanding the principles of sanitisation and ensuring that only relevant information is included in the report.

Where a source has been seen by other officers or criminals with the group of named individuals, not to name the source in the report might raise suspicions
If in doubt seek advice

Best Practice



Intelligence must not be influenced by personal feelings

Refer to ECHR duty of care

Safeguard intelligence collection techniques

To identify the time and place of a meeting may identify the source. It is possible that the information may only be known to the source. Should the information become known then the source could be compromised.

All police officers and police staff have a role to play in the management of police information and it is essential that every officer meets the responsibilities placed on them. When dealing with any type of police information you should always apply the basic principles of effective information management as detailed below:

- ☐ Always act within the framework of your force's IMS and any associated force policies and processes
- ☐ Always apply the four principles of data quality, namely that it must be:
 - o accurate
 - o adequate
 - o relevant
 - o timely
- ☐ Always apply the rules in relation to the security of information

Always ensure compliance with all relevant legislation including the Human Rights

Act 1998, Data Protection Act 1998, and Freedom of Information Act 2000

- When collecting information, ensure that you are aware, insofar as you are reasonably able, of the current intelligence requirements and also that the information is collected for a clearly defined policing purpose
- When recording information, ensure that you record it in the appropriate format, in compliance with the recording and data quality principles and make all necessary effort to ensure that person records are unique.

What is Provenance?



Provenance allows the source of intelligence to be protected in order to avoid any unnecessary risks to them



QTS – what does provenance mean and why is it important?

Provenance:

To Come From

Place of Origin

Ownership History

The term 'provenance' refers to the ability to determine the reliability and credibility of the information source and the value of the content of the information. It includes the risk to the source and subject, risk to the storage and use of the information.

It is important to establish the provenance as this is fundamental to evaluating individual information and intelligence records and action management. It is the provenance of the information that influences how a particular piece of information should be handled and disseminated and the subsequent action to be taken.

Provenance can be established through the interrogation of other information systems. For example, part of the information might be that John Kelly is using a red Ford Escort, XYZ 321 and a check on PNC might confirm that John Kelly is indeed the registered keeper of a red Ford Escort XYZ 321 - provenance is established.

When & Why do we use provenance?

- Needed to protect sources of information
- Duty of care

If the source is not protected then people will be reluctant to provide information.

If provenance is not used then there may be recriminations for the source.

We have a duty to protect the source.

Highlight that sources need to be recorded onto the system, police officers should **not** protect sources by saying that the information has come from the police officer.

The new system is a reliable way of protecting the source.

It is important to think about what risks there may be to the source as this will need to be recorded on the computer system.

Government Security Classifications

OFFICIAL

The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

SECRET

Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat factors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.

TOP SECRET

HMG's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.



Information has security classifications which indicate the sensitivity of the information (in terms of the likely impact resulting from loss or misuse), and the need to defend the information against threats.

These classifications operate within law – Official Secrets Act 1989, Data Protection Act 2018, & Freedom of Information Act 2000.

There are 3 levels of classification: Official, Secret and Top Secret.

As a Police Officer my majority of information handled will be treated as Official Classification

Definition:

ALL routine public sector business, operations and services should be treated as OFFICIAL - many departments and agencies will operate exclusively at this level.

This includes:

- The day to day business of government, service delivery and public finances.
- Routine international relations and diplomatic activities.
- Public safety, criminal justice and enforcement activities.
- Many aspects of defence, security and resilience.
- Personal information that is required to be protected under the Data Protection Act (2018) or other legislation (e.g. health records).

Storage of information and Intelligence

Information & intelligence can be stored in any suitable format. E.G paper records, computer records, audio tapes, video tape or photographs. Whatever system is used must be secure from unauthorised access



However, there are two important provisos, namely that the medium in which it is stored must be **durable** & the information must be **retrievable**



Durable means that the medium must be resistant to wear and decay. In the case of a computer system this would entail the contents of the system being backed up on tape or disc on a daily basis in case of a system crash or virus attack.

Retrievable means that the system in which the information is held must be searchable for individual records and those records can then be read, displayed on a screen or printed out.

The GDPR does not dictate how long we keep information for, however, we have policies in place within our forces, including the length of time fingerprints and DNA are kept on police systems if someone has been released with no charge. Look on the force systems in relation to retention as dependant on the information given to the police, will be dependant on how long it is kept and where.

Access and Retrieval

Records that have been retained must be stored in a format that allows them to be searched & retrieved. Police information & intelligence can only be accessed for authorised policing purposes & by personnel who are vetted & authorised to access protectively marked material. All police staff are personally responsible for ensuring that they comply with all relevant security policies & operating procedures



Archiving Information & Intelligence

Archiving is a form of retention, therefore any records that have been identified for disposal because they are inadequate or no longer necessary cannot be archived. However, a force can use archiving as a method of restricting access to those records that can be lawfully held



Disposal of Information & Intelligence

Disposal means the removal of information from **all** police systems, justified through the review process and to the extent that it cannot be restored owing to the fact that it can no longer be held lawfully.



Secure Disposal

The police duty of confidentiality in relation to police information applies from collection through the whole information management process and includes its final disposal. Therefore, all records must be disposed of in a secure manner and the method will depend on whether the records carry a protective marking.

When information records are disposed of, a record should be kept of the disposal which should contain:

Date of decision to dispose

Number of records

Whether records were considered inadequate or no longer necessary for a policing purpose.

The record of disposal must not contain any personal details of individuals.

Management of Information (Formerly MOPI)



Managing Information



August 2002

School girls Holly Wells & Jessica Chapman murdered in the village of Soham, Cambridgeshire



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

On Sunday, 4 August 2002, Holly Wells and Jessica Chapman, best friends both aged 10, had attended a barbecue at the Wells' family home in Soham. At around 6:15 pm they went out to buy some sweets. On their way back they walked past the rented house of Ian Huntley, a secondary school caretaker, in College Close. Huntley saw the girls and asked them to come into his house. He said that his girlfriend, Maxine Carr, their teaching assistant at St Andrew's Primary School, was in the house too. She had in fact gone to visit family in Grimsby, Lincolnshire. Shortly after the girls entered his house, Huntley murdered them.

Huntley's motive for killing Wells and Chapman may never be known, but minutes before seeing them he had reportedly slammed the telephone down on Carr following a furious argument; Huntley had allegedly suspected Carr of cheating on him. The police suspected that Huntley killed the girls in a fit of jealous rage. Huntley's mother also said this. The police found no evidence of premeditation

After the girls were reported missing, the police released photographs – taken only hours before their disappearance

Meanwhile, Huntley appeared in television interviews on Sky News and the BBC's regional news programme *Look East*, speaking of the shock in the local community. One reporter suggested to Huntley that he may have been the last person to speak to the girls before they disappeared, to which Huntley replied: "Yeah, that's what it seems like." Huntley said their disappearance was "absolutely" a mystery and that "while there's no news there's still that glimmer of hope, and that's basically what we're all hanging on to."

Carr, a teaching assistant at the school Huntley was also caretaker for, was interviewed by the press as well. She showed a reporter a thank-you card Wells had given her on the last day of the school year. Carr said: "She was just lovely, really lovely" and urged the missing girls to "just come home". The police immediately noticed that Carr was referring to Wells in the past tense, although she had not been reported dead.

On 16 August, 12 days after the girls went missing, Huntley and Carr were first questioned by police and agreed to give witness statements during seven hours of questioning before being released. That night, police searched Huntley and Carr's home, as well as the grounds of Soham Village College, and recovered items of "major importance" to their investigation. Although it was not made public at the time, the items recovered from the school grounds were clothes matching those the girls were last seen wearing, including their Manchester United shirts. Huntley and Carr were arrested in the early hours of 17 August on suspicion of murder. This was the first time that the police admitted that they feared the girls were now dead.

The girls' bodies were found in a ditch near the perimeter fence of RAF Lakenheath in Suffolk, about six miles from Soham, on the afternoon of 17 August, less than 24 hours after their clothing had been discovered in the grounds of Soham Village College. The girls had been missing for 13 days when their bodies were found, with police stating that both corpses were "severely decomposed and partially skeletonised". Huntley had set them alight in a bid to destroy forensic evidence. Dr. Patricia Wiltshire was however able to identify the time the bodies were placed and provide evidence that proved Huntley to be the killer, based on analysis of the soil environment

MOPI



Ian Huntley



Maxine Carr



Ian Kevin Huntley was sentenced to two terms of life imprisonment, with the High Court later setting a minimum term of 40 years.

His girlfriend, Maxine Ann Carr, was the girls' teaching assistant at St Andrew's Primary School. Carr had provided Huntley with a false alibi and was sentenced to 21 months in prison for perverting the course of justice.

5 min video to be played regarding Ian Huntley.

Can also be found within the lesson material folder

Bichard Inquiry Main Points

Registration scheme
for everyone
working with
children

National IT system

Investment in PNC

Enhanced criminal
checks for those
working in schools

National Code of
Practice

Guidance for social
services when
referring cases to
police involving
under age sex



QTS – does anyone know what any of the recommendations were as a result of the Bichard inquiry?

The Management of Police Information (MoPI)

MoPI (now Managing Information), was introduced in 2005, as a result of the recommendations of the Bichard enquiry report. It is being implemented by all police forces in England and Wales.

Sir Michael Bichard's inquiry into the Soham murders lead to recommendations for the improvement of the management and sharing of information and intelligence by Police Forces at national and local levels.

Information needs to be accurate, relevant and accessible. Managing Information ensures that all information is managed in a consistent way. The code and guidance make sure that this happens.

"The transfer of information between forces is now paramount. It's the lifeblood of the organisation. We need to make sure that the intelligence and information which we hold on people is fully accurate and that the transfer of this between forces actually exists and happens." Gary Thompson, Superintendent, Gloucestershire

Relevant guidance, including:

- Managing Information
- APP Information Management <https://www.app.college.police.uk/information->

management-index/

- Government Security Classifications (GSC)
- Information Sharing Agreements (ISA)

We will discuss these through the session and have an understanding of how they can assist in information and intelligence gathering.

Following Huntley's conviction it emerged that Huntley had in fact been known to both the police and social services over a number of years. Between 1995 and 1999 he came to the attention of Humberside Police in respect of allegations of eight separate sexual offences involving young girls. During the same period he came to the notice of Humberside Social Services in respect of three separate complaints involving young girls, none of which were notified to the police. As a result of various failings in the way in which that information was handled by the agencies involved, none of these instances were revealed in Cambridgeshire Constabulary's Record search in 2001.

The then Home Secretary, Rt. Hon. David Blunkett MP, ordered an inquiry into child protection measures, record keeping, vetting and information sharing in Humberside Police and Cambridgeshire Constabulary. That inquiry opened in January 2004 chaired by Sir Michael Bichard.

The key findings of the inquiry found:

1. A failure to record information properly - ignorance at all levels of how to create records on force data bases and inadequate guidance and training on intelligence systems.
2. A failure to submit intelligence reports - because officers did not realise their importance and in some cases it was considered unnecessary as other documents had been submitted.
3. A failure to review information - there was no 'weeding', 'reviewing' and planned 'deletion' of records. There were 'automatic deletions' of records regardless of the importance of the information contained in the records.
4. A failure to share information between police and other agencies - lack of any information sharing protocols between agencies or where they did exist, a lack of knowledge of them.
5. The inquiry concluded that weaknesses were not confined to a particular force, individual or set of circumstances. Weaknesses existed throughout the whole information management process.

Recommendations

The inquiry made a total of 31 recommendations some of which relate to the Home Office, Social Services and other agencies. However, there are four which have direct relevance to the police and the management of police information.

1. Development of a Code of Practice for the management of police information (MoPI)
2. The Code must set out the key principles of good information management

3. The Code must create standards for systems, accountability, training, resources and audit with regard to information management
4. The Code must have particular regard to the review of intelligence in the case of sexual offences.

Managing Information Guidance

The Code of Practice on the Managing of Information states:



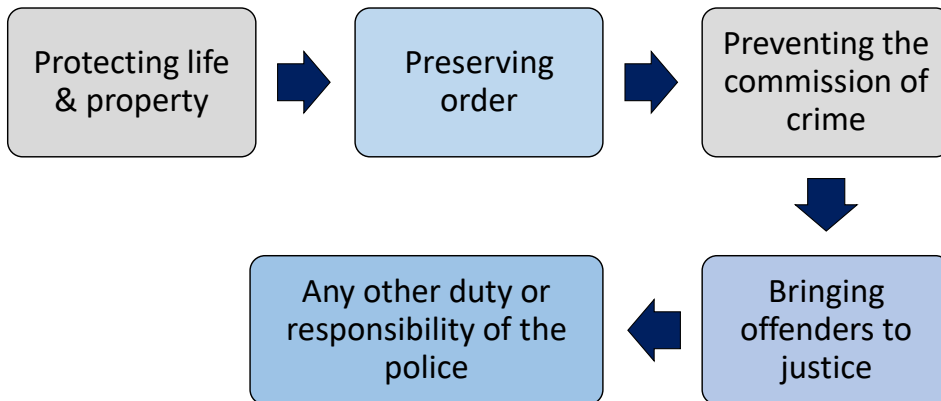
Information gathered by the
police must be :-



**For a policing purpose
And
Managed lawfully**



Policing purpose refers to.....



QTS – what is a policing purpose?

The principle behind Managing Information is that where data is gathered or stored by the police, it must be done for a lawful purpose.

Managing Information

Gathering & storing
information &
intelligence

Sharing
information &
intelligence

Legal
considerations

Crime & Disorder
Act 1998

Computer Misuse
Act 1990

Criminal Procedure &
Investigations Act 1996

Data Protection Act 2018/
General Data Protection
Regulation (EU) 2018/679
(GDPR)



Information/intelligence gathered must be stored as accurately as possible – the 3X5X2 system assists in categorising how accurate (or inaccurate) the officer thinks it is.

Crime & Disorder Act 1998 states partners are **required** to share information. This is overcome by information-sharing protocols, which are written and signed by partners allowing the sharing of data relevant to crime and disorder under the strict guidelines of the protocols.

Information Sharing Agreements are formal agreements for the exchange of information and intelligence between the Police and its partners. The shared information is typically used to prevent, detect, and/or reduce crime.

Computer Misuse Act 1990 outlines offences of accessing data you're not entitled to see (such as PNC/Intel systems) and a more serious offence of using that data to commit a crime.

The Criminal Procedures & Investigations Act 1996 requires the police to Record, Retain and Reveal any material gathered during a criminal investigation (not just data) and disclose anything relevant to the investigation which may weaken its own case or strengthen that of the defence.

The implications of gathering inaccurate data will be felt if the case collapses when the information is disclosed to the defence – but the police could also be

in breach of the MOPI guidelines. This could also lead to discipline issues for officers & police service

Police officers are not allowed to disclose data held on computers to anyone not entitled to receive it (such as members of the public or partners).

Data Protection Act 2018/General Data Protection Regulation (EU) 2018/679 (GDPR):

This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. In essence it is the protection of data to those within the EU and the European Economic Area (EEA); and will also address the personal data to outside of the EU and the EEA. Controllers and processors of personal data must put in place *appropriate technical and organisational measures* to implement the **data protection principles**. Business processes that handle personal data must be designed and built with consideration of the principles and provide safeguards to protect data e.g. fully anonymising the data where appropriate.

Review for Retention

Reviewing information held by forces to determine its adequacy & continuing necessity for a policing purpose is a reliable means of meeting the Data Protection Act 2018



Review procedures should be:

- practical
- risk focused
- able to identify valuable information
- as straightforward as is operationally possible.

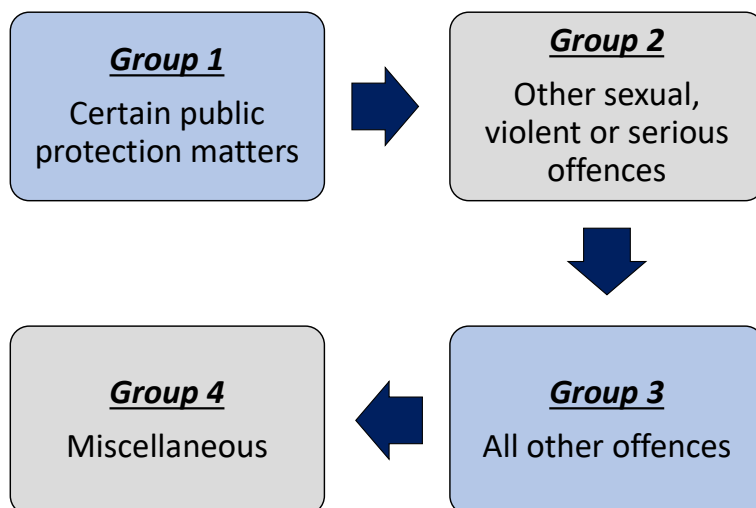
The police service should have standard procedures in place for reviewing records and making accountable decisions on the retention or disposal of information. Review procedures ensure that information retained by the police service is held lawfully, and may help to prevent forces being overloaded by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

All person records held by the police service are subject to:

- an initial review and evaluation
- any necessary triggered reviews
- scheduled reviews.

For audit and supervision purposes, a record must be kept of every review undertaken, irrespective of whether it results in any alterations or disposal.

Timeline for Retention



Group 1 – certain public protection matters

Information is placed within this group until a subject has reached 100 years of age (calculated using the subject's date of birth). This information should be reviewed regularly, ie, every 10 years, to ensure that it is adequate and up to date

Group 2 – other sexual, violent or serious offences

This group also includes all specified offences that are not serious offences as defined in the [Criminal Justice Act 2003](#). A full list of these offences is recorded on the PNLD.

Information relating to [sexual](#), [violent](#) or [serious](#) offences that are not listed as serious specified offences in the CJA can be retained only for as long as the offender or suspected offender continues to be assessed as posing a risk of harm, using the NRAC.

After every 10-year clear period, these records should be reviewed and a risk-based decision made on whether they should be disposed of or retained. This group includes any information related to persons convicted, acquitted, charged, arrested, questioned or implicated with an offence within this group. If the individual in question continues to offend or is implicated in continued offending, records relating to them must be retained. In these circumstances, however, the absence of a clear period means that forces do not have to conduct a scheduled review or justify the continued retention of such records. The triggered reviews process ensures that records relating to this group of offenders remain adequate and up to date.

Sexual offences



For the purpose of information management, a sexual offence is any listed in [Schedule 3](#) of the Sexual Offences Act 2003.

Violent offences

For the purpose of information management, a violent offence is any of those specified as such in the current [Home Office counting rules for recorded crime](#).

Serious offences

For the purpose of information management, a serious offence is any offence detailed, recorded or listed as such on the PNLD.

Group 3 – all other offences

Records relating to people who are convicted, acquitted, charged, arrested, questioned or implicated for offending behaviour which does not fall within [group 1](#) or [group 2](#) are dealt with in group 3. Records that fall within this group do not necessarily have to be reviewed. Forces may opt to use a system of time-based, automatic disposal for classes of information in this group.

Forces which opt to use time-based disposal for all or a proportion of their group 3 records must observe the following principles:

the criteria by which forces decide which group 3 records to review and which to automatically dispose of must be outlined in the [information management strategy](#)

the risk of disposing of records without review lies with the chief officer

all records subject to time-based disposal must still be retained for an initial six-year period

forces must have a mechanism for identifying those group 3 individuals who continue to reoffend or who are implicated or suspected of being implicated in offending, and retain records relating to them

forces must have a mechanism for identifying those individuals who have demonstrated a capacity for inflicting serious harm, using the [NRAC](#) and by flagging records relating to them for [exception reviews](#)

any group 3 records that forces wish to retain for longer than six-year [clear period](#) must be reviewed at five-yearly intervals and risk assessed using the NRAC.

Group 4 – miscellaneous

This group contains information on undetected crime, intelligence products, missing persons, and victims and witnesses.

Undetected [group 1](#) offences – records should be retained for a minimum of 100 years from the date reported to the police. Other records of undetected offences should be retained for a minimum of six years from the date reported to the police. Forces should be mindful that these are minimum periods and that they may keep undetected crime records for longer if they feel it necessary. There are no additional requirements to review these records above and beyond the requirements imposed by relevant investigative guidelines.

Intelligence products – should be reviewed in accordance with the [review schedule guidance](#). The type of criminal activity being examined determines the length of time between reviews.

Missing persons – information relating to open missing persons cases should be retained until the person is located. For cases of missing persons who have subsequently been located safe and well, information should be retained for a minimum of six years. If this initial six-year period is clear, ie, the individual does not go missing again and there are no subsequent indications of abuse, domestic violence or other factors that might place the individual at risk, the record should be disposed of.

Victim and witness information – should be retained for an initial six-year clear period or for the length of time required by the [Criminal Procedure and Investigations Act 1996](#), if this is longer. Beyond this point, the decision about whether to retain victim and witness details should be made on a case-by-case basis. Records should be retained if they provide detail of an offender's MO or any relevant risk factors. Witness statements generally fall into this category. If, however, this detail is duplicated elsewhere, it could be deleted from the system.

In all cases victim and witness details should be handled with care and in accordance with their right to privacy.

In circumstances where a victim or witness is recorded on police systems as an offender or suspect in another matter, their details should be retained and reviewed in accordance with the incident in which they are the person of interest.

The Authorised Professional Practice (APP)

The Authorised Professional Practice (APP) on Managing Information provides the framework for the management of police information & supersedes the ACPO 2010 Guidance which has been decommissioned. The APP for intelligence management does the same & is intertwined with information management

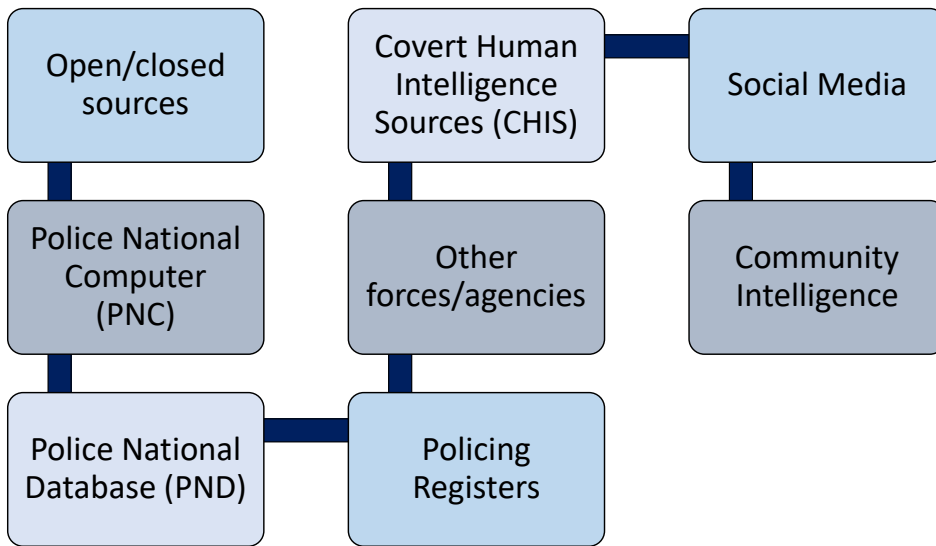


<https://www.app.college.police.uk/information-management-index/>

This is a hyperlink to the College of Policing APP website – this hyperlink can be provided to the students to log on and have a look so that they are aware of the site and how to use it.

It outlines what processes and procedures the police service must have in place for the management of police information. How these are applied is determined at force level and must be fully detailed in the force's Information Management Strategy (IMS) as well as in force policies.

Sources of Information and Intelligence

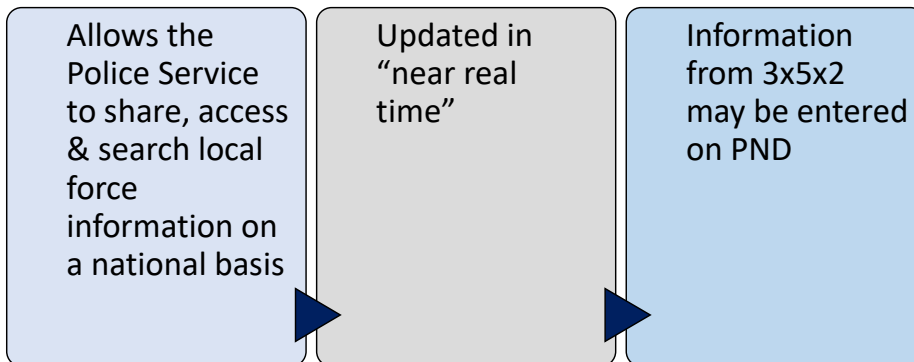


Information and intelligence is the life-blood of the police service and it should be considered not just as a local but a regional and national policing resource. Information collected in one area of a force may have a value to another or to another force or agency, eg, the National Crime Agency (NCA) or Social Services.

Traditionally, however, information has been held in discreet business areas and was not capable of being searched. This has resulted in the ineffective and difficult linking together of people, objects, locations and events, even within the same force. This problem had been magnified at regional and national levels because of the lack of common standards for information recording and evaluation, and as a consequence the sharing of information within the police service and with key partner agencies was, in some cases, impossible and in others unnecessarily complicated.

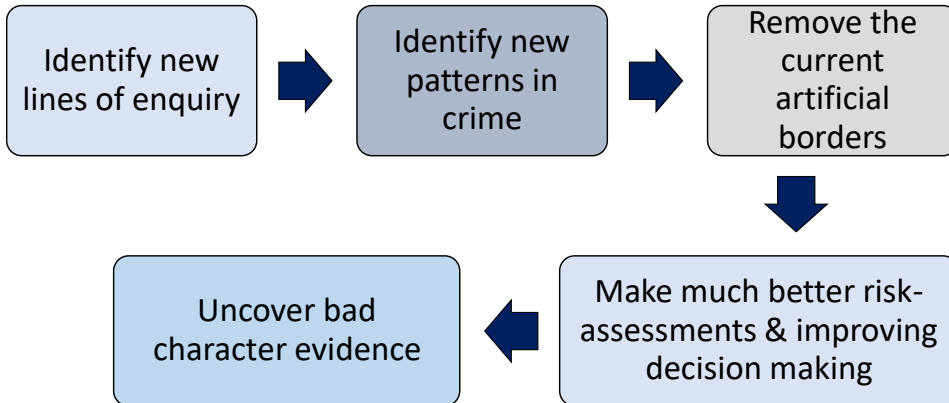
The purpose of managing information effectively is therefore to facilitate effective and efficient policing everywhere.

Police National Database (PND)



Sharing of all intelligence information between forces i.e officer in Swansea puts a log in about someone who lives in Llanelli but the information relates to something in the Swansea area our intelligence system would not show that log but a PND check would. If you suspect that there may be cross border information you should go through to the FCC and also request a PND check. We do not have access to this system without separate training and access to the database.

PND Benefits



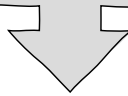
QTS – what are the benefits of the PND?

PND

Witness data should **not** be included on the PND but some victim data will, in limited cases be available

POLE Searches:

PND searches operate on 4 areas that give structure to the speed & quality of the information that can be searched



People

Objects

Location

Events



Information Sharing



Effective policing is
reliant upon the lawful
sharing of information
with the police service
itself, with other
agencies, with individuals
& with the general public



Benefits of Sharing Information

The lawful sharing of information has a number of benefits for the police service:

A 2 way process with information flowing from & to the police service.
Helps provide improved public services. Enables links to be made between people, objects, locations & events using data that might not have been available to the other party without it being shared

Increased openness among partner agencies builds confidence & trust in the police service

It allows police & partners to make better informed decisions on how best to protect the public

Formalised processes increase confidence of individual officers & staff to lawfully share information. Increases expertise & professionalism



QTS – what are the benefits of sharing information?

Sharing Information within the Police Service

Subject to any handling codes applied to the information, police forces can freely share information with one another if it is for a policing purpose (see the section covering NIM for an explanation on handling codes)



You have a responsibility to ensure the security of information & you must record your information sharing decisions in accordance with your own force policy. It is vitally important that you submit intelligence in an 'unsanitised' format



As previously explained in slide 21, when an officer submits intelligence in an 'unsanitised format' the LIO will conduct a process called 'sanitisation' with the information they receive from the officer. They will remove information from the officer's report which explicitly or implicitly identifies a source or an address which is sensitive.

Sharing Information Outside the Police Service

Before information can be shared with bodies outside the police service there must be one of the following:

Statutory obligation

A specific legal obligation or requirement to disclose police information to another party

Statutory power

A specific legal power, but not an obligation to share police information with another party

Common law

If there is no statutory obligation or power to share information then a common law policing purpose must be established



Before information can be shared with bodies outside the police service there must be one of the following:

Statutory obligation - a specific legal obligation or requirement to disclose police information to another party. For example:

- Disclosures from the Disclosure and Barring Service (DBS) for vetting purposes
- Road Traffic Act 1988 - such as exchange of name and address after a collision
- Court Order such as a Disclosure Order, or

Statutory power - a specific legal power, but not an obligation, to share police information with another party. For example:

- The Children Act 1989
- The Crime and Disorder Act 1998
- The Criminal Justice Act 2003, or

Common law - if there is no statutory obligation or power to share information then a common law policing purpose must be established. For example:

- The Notifiable Occupation Scheme (Home Office Circular 6/2006), which relates to professions or occupations that carry a special trust or responsibility.

The decision to share police information

Once a policing purpose has been established then you need to conduct a risk

assessment as to what information to share. The assessment must carefully balance the data protection and human rights conditions against the policing purpose. Any information that is shared must be necessary for the purpose for which it is being shared.

Police forces should actively seek opportunities to share non-personal information such as providing details of burglaries in a specific area with the relevant Neighbourhood Watch group. However, the sharing of personal or sensitive personal information requires additional safeguards.

Information Sharing Agreement (ISA)



The purpose of an ISA is to formalise arrangements between organisations which need to share information on a regular basis



An ISA may be an existing national agreement between agencies or it may be a purely local arrangement



Key responsibilities for information sharing - a summary

1. Purpose - ensure the information being shared meets a policing purpose, or can be lawfully disclosed for a statutory purpose and is proportionate and necessary.
2. The information - ensure the information is relevant, accurate and adequate for the purpose for which it is being shared.
3. Legal requirements - ensure that when personal or sensitive personal information is shared, the requirements of the Data Protection Act 1998, the Human Rights Act 1998 and the common law duty of confidentiality have been met.
4. Risk assessment - apply protective marking to the information being shared under the GCS where applicable. Otherwise carry out a risk assessment where the sharing is with partners in the voluntary or private sectors that do not have a statutory purpose to share information.
5. Record the decision - you are responsible for recording any decisions to share or not to share information on the relevant system within your force. The decision must be auditable at a later date (remember the support offered to you under the National Decision Model).
6. This will also help to flag any necessary markers and associations and/or behaviours that are of note

Information Sharing Agreement (ISA)

What is an ISA?

They are formal agreements between organisations that are sharing personal data. They explain why data is being shared & set out the principles & commitments organisations will adopt when they collect, store & disclose personal information about members of the public

Protocols/agreements also explain when information can be shared. Without such formal agreements, public organisations may find themselves falling short of common standards. Also, there may be confusion over responsibilities – both within & between organisations



Hand Out:

Other law based agencies that work alongside police

E.g., Interpol, Europol, Immigration etc.

When Can Information Be Shared?

There are several types of circumstances where information can be shared

Emergency situations

Routine

Ad-hoc

If you genuinely believe that imminent harm will come to someone if you do not disclose information immediately, you should release the information. The DPA does not put privacy above people's welfare



There are several types of circumstances where information can be shared.

Emergency situations

In an emergency situation most organisations will share information without asking for further details. **The Data Protection Act allows the processing of personal data if it is in “the vital interests” of the data subject or any other person;** usually this would mean that someone was at immediate risk of harm. For example, in cases of life or death, such as where an individual's identity and/or medical history is disclosed to a hospital's A&E department treating them after a serious road accident. There should be conditions of real urgency that necessitate the immediate sharing of data without reference to proper procedures. This method of sharing data must not be abused e.g., by the requester exaggerating the gravity of the situation.

Routine

Another circumstance is the routine and systematic dissemination of information between partners for the purposes of a particular initiative. These initiatives can be fairly broad in aspect and include tackling anti-social behaviour, child protection, and social care. Information sharing is vital to these initiatives and protocols should be drawn up outlining the process and method of sharing data. This is likely to happen on a regular basis and in a controlled manner in a multi-agency setting. There will usually be named individuals through whom all requests should be made.

Ad-hoc

In many cases requests are made on an ad hoc basis between organisations and individuals. This covers a very wide range of possibilities and is much more complicated.

In a non-emergency situation a request for personal data should be made via a Section 29(3) form. This will allow the receiving organisation to consider the request and either provide the information or refuse to release it. If the request is refused but the information is still deemed to be necessary then a court order can be applied for. Asking for a court order is seen as a safer option for some organisations as a complaint can be made by the data subject if they feel their data has been shared unlawfully.

Requests from other organisations should state the authority or power that allows the information to be shared, eg the Child Support Agency has several powers that oblige organisations to disclose data. Any request should state that power and should be made under Section 35(1) of the Data Protection Act. These type of requests should always be made in writing with time for the receiving organisation to consider them.

Retrospective Facial Recognition is a technology that can assist the Police in identifying an unknown suspect from a CCTV or other image that has come to light as part of a criminal investigation. The technology is used to check if the image matches any of the photos that we hold of people who have previously come into police custody. All three Emergency situations, routine and ad-hoc processes can give rise to the use of facial recognition technology

Failing to Share Key Information

The Fiona Pilkington case had its origins in harassment & ASB. Fiona & her daughter suffered frequent & sustained local disorder, often directed at their home over a period of several years. This was reported to the police but *'incidents were too often dealt with by police officers in isolation & with an unstructured approach'* (IPCC 2011). This & other factors such as not identifying the family as vulnerable & not recognising the harassment & ASB as targeted hate crime caused frustration. Fiona eventually took her own life & that of her disabled daughter Francesca



Feedback

How to provide post incident feedback

The purpose of debriefing is to identify good practice & areas for improvement, which could include organisational learning & joint organisational learning (see JOL via JESIP for more information) The gold, silver or bronze commander should establish at an early stage, the debriefing arrangements required & identify who should be responsible for compiling & assessing any debriefing material generated.



Pressure on operational staff can lead to debriefing being overlooked. This should not be allowed to happen as effective debriefing will ultimately minimise bureaucracy, streamline current procedures and reduce demands on operational staff.

See the Knowledge Hub [Specialist Operations National Structured Debrief community](#) for identified good practice and areas of learning. Note – the reader must already be logged into the Knowledge Hub to access the link.

