Collection and recording

This page is from APP, the official source of professional practice for policing.

First published 23 October 2013 Updated 7 September 2023
Written by College of Policing
15 mins read

Collection, accurate assessment and timely analysis of information are essential to effective and efficient policing.

Collection

This is the start of the information management process. It affects all other stages of information management, from how the information is recorded to how long it will be retained. A force **information management strategy (IMS)** allows information requirements to be set and so determines the information that needs to be collected.

Information collected for one policing purpose may have value to another. All police information should, therefore, be treated as a corporate resource.

Means of collecting information

The way in which police information is collected may lead to specific requirements for its recording and use, as is the case with information covered by the **Regulation of Investigatory Powers Act 2000**.

It is essential that information is collected, recorded and evaluated in a consistent manner across organisational and force boundaries. It should not matter where the information originates from, and it should be available to support policing purposes across the country.

Information is collected in one of three ways:

- routine collection
- **tasked information**
- volunteered information

Routine collection

This is information collected as part of routine operational policing activity. Much of it is relevant only for the specific policing purpose for which it was collected, but some will prove to be relevant to an entirely different policing purpose. Information is generated from all policing activities, for example:

- responding to incidents
- arrests
- targeted patrol
- stop and account
- stop and search

Volunteered information

This type of information is usually collected from the general public, community contacts and partners. It refers to any information received which has not been obtained by routine or tasked collection. As such, it:

- may not necessarily relate to a specific tasking or intelligence requirement
- is usually received because people want something done with the information
- can refer to information that the police have requested
- can be regarded as intelligence

It can be received in any format, at any time, and includes:

- any public contact through command and control or crime systems
- information from voluntary organisations, for example, Neighbourhood Watch
- anonymous information, for example, from Crimestoppers or the anti-terrorism hotline
- information from partner agencies, for example, social services for a child protection matter

Key roles in collection

Managers ensure that:

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

Supervisors provide:

- briefings and tasking to staff deployed to collect information
- the opportunity for debriefing operations

Users ensure that:

- they are aware of the current intelligence requirements
- information is collected for a policing purpose, in line with the **Data Protection Act 2018**, **data quality principles**, the **Human Rights Act 1998** and the **Freedom of Information Act 2000**

Recording

Police information can be recorded in different formats and held in different business areas, according to the purpose for which the information has been recorded, for example:

- domestic abuse
- child abuse investigation
- public protection
- the violent offender and sex offender register (ViSOR)
- missing persons
- **intelligence**

The force IMS should specify where information is recorded.

Different formats can be used, and information can be held in different business areas, according to the purpose for which information has been recorded, for example:

- **crime recording**
- **case and custody**
- **incident records**
- **firearms licensing**
- **Police National Computer** (PNC)
- **intelligence systems**

Information from key business areas (for example, crime, intelligence, domestic abuse, child abuse and custody) should be uploaded onto the Police National Database (PND) on a regular basis.

Crime recording

Forces should comply with the national crime recording standard (NCRS) and the Home Office counting rules (HOCR) when recording crimes.

Each force has a crime registrar (FCR) who acts as the final arbiter for the interpretation of the NCRS and the HOCR, and for the quality assurance process. Any questions on the correct classifications or process should be directed to the FCR.

Many crimes are initially reported and recorded as incidents. Incident recording is set out in **Association of Chief Police Officers (ACPO) (2011) National Standard for Incident Recording (NSIR)**.

For further information see Home Office guidance on **Counting rules for recorded crime.**

National crime recording standard

The NCRS promotes consistency between police forces in how to record crime and in providing a victim-orientated approach to crime recording. This standard has three basic principles.

- The police register an incident report for all reports of incidents (whether from victims, witnesses or third parties and whether crime related or not).
- An incident is recorded as a crime (notifiable offence) if – on the balance of probability – the circumstances as reported amount to a crime defined by law, and there is no credible evidence to the contrary.
- Once recorded, a crime remains so unless there is additional verifiable information to disprove it.

Crime reports record details which include:

- name
- time, day, date of incident
- time, day, date of recording
- how the crime was reported
- who reported the crime and the method of reporting
- location
- modus operandi – this field should be as complete as possible because it often forms the basis for identifying suspects

Incident record

This report is defined as any communication from any person, by whatever means, about a matter that comes to police attention and which is required by the NSIR to be recorded.

There are a number of minimum data standards to be complied with when recording information on an incident record:

- time and date the report was received
- method of reporting
- time and date the report was recorded
- an incident unique reference number (URN)
- details of the person making the report (name, address and telephone number)
- sufficient information to describe the location and nature of the report
- opening and closing category
- time and date of initial and closing classification

For further information see Home Office guidance on **Counting rules for recorded crime.**

Case and custody

Custody systems used in the detention process contain prisoners' personal and arrest details. A case system manages all aspects of case file preparation following the decision to instigate proceedings. This includes the management of defendants and witnesses.

Several different case and custody systems are used in the police service. One example is the national strategy for police information systems (NSPIS) case and custody, which is designed to interface with crown prosecution service systems and enable communication across all agencies in the criminal justice system.

National firearms licensing management system

Information about legally held firearms is held on this system, and includes:

- data on persons holding a shotgun – name, address, date of birth, certificate number, conditions of licence, serial numbers

- section 1 firearm – the same details as above and also ammunition
- registered dealers – name, address, licence information and which explosives can be held (this information is linked to the PNC)
- revocations and refusals

Considerations

Recording police information in accordance with national standards:

- ensures that all police information is held in accordance with the law
- supports decision making through the **intelligence** process
- provides an auditable **decision-making** process
- corroborates other related information
- allows information to be shared

Principles

There are key principles which apply, regardless of the format and business area where police information is held. The person recording the information must ensure that they have regard to these principles.

- A record must have been created for a **policing purpose.**
- All records must comply with the **data quality principles.**
- A record of police information is the start of an audit trail and must identify who completed the record, when it was completed and for what purpose.
- Before recording information, checks should be made in other business areas to see whether the information is already held, thereby avoiding unnecessary duplication.
- If information is recorded on an individual who is the subject of an existing record, the record should reflect this.
- If it becomes apparent that the information being recorded is connected to other information, it must be appropriately linked.
- Police information must be recorded as soon as is practicable, in accordance with the standards relating to the business area in which the information is held.
- Consideration should be given to applying the appropriate government security classification.

- Where appropriate, the source of the information should be recorded to ensure accuracy and to assist in requesting further information.

Data quality principles

All police information must conform to data quality principles. It must be:

- accurate – care must be taken when recording information and, where appropriate, the source of the information must also be recorded. If there is any doubt over the authenticity of the information, clarification must be sought from the source. Inaccurate information must be corrected as soon as possible. In ensuring accuracy, it is important not to delete historic information that may be significant (such as details of previous addresses).
- adequate – recorded information must be sufficient for the policing purpose for which it is processed. The nature of the event determines the information that is relevant. All recorded information must be easily understood by others.
- relevant – information recorded must be relevant to the policing purpose. Opinions need to be clearly distinguished from fact.
- timely – information must be promptly recorded into the relevant business area, in accordance with agreed timescales.

These data quality principles are reflected in the **Data Protection Act 2018 part 3, chapter 2, s 37 – 39**.

Categorising police information

Categorising records allows information to be arranged so that a force knows which information is held where. It also helps to identify gaps in the information needed to support the force **IMS** and intelligence requirements.

Records can be categorised in terms of people, objects, locations and events (POLE). Person records present most risk for offenders, victims and sources. Categorising information also enables compliance with the Data Protection Act 2018.

Person records

In order to create a person record, every effort should be made to establish a person's identity. The greater the detail, the greater the likelihood the record will be unique. This should, however, be proportionate to the reason for recording the information.

The **Data Protection Act 2018** requires forces to register their data protection officer with the Information Commissioner's Office to notify that personal information is held and used for specific purposes. It also requires forces to have an Information Charter (or privacy notice) to inform individuals of the types of personal data they process, the purposes for which they are processed, and any recipients it may be disclosed to. The details of the data protection officer are included in a public register, unless they are exempt.

When creating a person record, it should contain, as a minimum, one of the following:

- forename
- family name
- partial name
- nickname
- alias

A description has to include a name in order to create a person record. Other desirable basic fields to add to a person record are:

- age (date of birth)
- sex
- race/ethnic origin
- height

Establishing a person's identity

It is desirable that person records are linked to a URN. Having a URN for records held within PND business areas allows for all the information known about a person across the different business areas to be linked. This means information is managed more effectively both at force and national level.

The **Police National Computer (PNC)** can be used to help confirm a person's identity, and it should be checked to establish whether a person is already known to the police service. PNC name checks should not be the only method of verification and cannot be relied on solely for correct

identification. Biometric data, such as fingerprints, DNA or recorded marks and scars, should be used to confirm a person's identity where possible. If a PNC record can be accurately linked to a person record, a cross-reference should be made on the person record to the PNC ID.

The PND enables forces to search person records nationally and provides forces with immediate access to up-to-date information drawn from local crime, custody, intelligence, child abuse and domestic abuse systems.

Key roles in recording

Managers ensure that:

- data quality is treated as a priority
- there is the ability to link and cross-reference information across the different business areas
- staff responsible for recording police information are suitably trained

Supervisors:

- regularly dip sample records to ensure that they comply with data quality and recording principles
- ensure that staff are recording information in the appropriate format
- provide feedback to staff on record creation

Users should:

- record information in the appropriate format
- record information in compliance with the recording and data quality principles
- make all necessary efforts to ensure person records are unique

Government security classification

Those handling police information have a responsibility to value and safeguard all information they send or receive. Where necessary, appropriate classification and measures should be clearly identified in order to enable sharing and to protect from loss, damage or unauthorised and inappropriate access to the information.

Classification ensures that police information is handled appropriately in order to protect individual rights in accordance with the law **(Data Protection Act 2018, part 3, chapter 2, s 40)** and with

respect for the wider public interest.

The **Government Security Classification (GSC)** provides:

- an improved, simplified and pragmatic common approach to assessing the value of and classifying information
- a flexible approach to information security and sharing information with government agencies and trusted partners
- modernised IT systems that are developed and operated to a common standard
- improved security by encouraging individuals to take personal responsibility for thinking about the information they produce and handle
- an assurance that sensitive information will receive the protection it needs so that it is only ever disseminated on a ‘need to know’ basis, particularly outside the police service

Documents and/or assets previously classified under the Government Protective Marking Scheme (GPMS) do not need to be reclassified. Documents which are routinely reviewed (namely, policies, procedures and information sharing agreements) should be reclassified under the new grading as and when they are next reviewed.

Business area leads will review the GSC and are responsible for implementing any relevant business change.

For further information, see:

- **e-learning package – An introduction to Government Security Classification (GSC)**
- **Cabinet Office (2023) Government Security Classifications Policy**

Key principles

There are four key principles that define the GSC.

- Principle 1 – This is the default principle. There is no need to routinely mark documents or emails as OFFICIAL.
- Principle 2 – Where it is considered that the content needs marking, it can be marked as OFFICIAL. However, the originator must state why they have marked it OFFICIAL, and consider whether they need to provide handling conditions.

- Principle 3 – Where there is a ‘need to know’ and further security control measures are required to protect the information, the information must be clearly marked as OFFICIAL-SENSITIVE. Originators must state why it has been marked as OFFICIAL-SENSITIVE and must also apply handling conditions and network control measures.
- Principle 4 – SECRET/TOP SECRET are for business as usual.

Considerations

Information that does not meet the criteria for SECRET or TOP SECRET is automatically classified as OFFICIAL and there is no need for it to be marked.

Prior to classifying information, the following should be considered.

- Does the information require protecting? If so, why? Could the information:
  - have a detrimental impact on an investigation?
  - cause a risk to life and/or safety?
  - be breaching legislation restrictions (including the **Data Protection Act 2018)**?
  - have an impact on security or intelligence-led operations?
  - have a detrimental impact on the originating organisation or the police service?
- What would be the consequence if the information went to the wrong person?
- Who are the recipients of the information?
- How is it being sent?
- How should the recipient handle the information?
- How should the information be protected, if required?

Government security classification model

Although there is no direct correlation between the new GSC and outgoing GPMS, the diagram below demonstrates how GSC compares with GPMS. It also identifies the three new categories and the use of OFFICIAL-SENSITIVE within OFFICIAL.

By default, all material will be classified as OFFICIAL unless the information warrants any consideration for higher marking and handling restrictions.

OFFICIAL

The majority of information created or processed by those working with police information is classified as OFFICIAL. This includes routine communications and documents such as emails, operating procedures and press releases that are not subject to a heightened threat. Information that is OFFICIAL does not need to be classified.

Within OFFICIAL, there is a greater emphasis on people, process and procedural assurances to address the fundamental risks.

OFFICIAL-SENSITIVE

Some OFFICIAL information is considered sensitive and could have damaging consequences if lost, stolen or published in the media. OFFICIAL-SENSITIVE is a descriptor within OFFICIAL. It identifies that the information requires safeguarding against unwarranted disclosure and will typically require more rigorous handling controls. It can be applied where the originator of the information (either document or email) considers that there is a requirement to reinforce the ‘need to know’ principle.

Content classified as OFFICIAL-SENSITIVE will be of a sensitive nature. Damaging consequences for an individual (or group of individuals), an organisation or forces could occur if there was unwarranted disclosure of the information.

The use of OFFICIAL-SENSITIVE should be by exception and should not be a default position. It should not become the norm for information that would have previously been classified as CONFIDENTIAL or RESTRICTED under GPMS.

All material marked OFFICIAL-SENSITIVE must include handling conditions. Reference on how to add these conditions should be outlined in force policies.

SECRET

Information categorised as SECRET is very sensitive and justifies heightened protective measures to safeguard against determined and highly capable threat actors. It should be used where information disclosure may compromise and seriously damage military capabilities, international relations or the investigation of serious organised crime. This information could cause:

- a threat to life directly leading to limited loss of life
- disruption to emergency service activities that requires emergency powers to be invoked (for example, military assistance to the emergency service) to meet expected levels of service
- major, long-term impairment to the ability to investigate serious crime (as defined in legislation)
- a number of criminal convictions to be declared unsafe or referred to appeal (for example, through persistent and undetected compromise of an evidence-handling system)

It is likely that most police staff will only occasionally have access to SECRET material and usually only in controlled circumstances. Enhanced security vetting is required for regular access.

TOP SECRET

Information categorised as TOP SECRET is the most sensitive information requiring the highest levels of protection from the most serious threats. This information could compromise and cause widespread loss of life or threaten the security or economic wellbeing of the country or friendly nations. In addition, this information could:

- directly threaten the internal stability of the UK or friendly countries, leading to widespread instability
- cause major, long-term impairment to the ability to investigate serious organised crime (as defined in legislation)
- cause the collapse of the UK judicial system

It is highly unlikely that most police staff will ever be granted access to TOP SECRET material. If so, it will be in very specific circumstances. Highest-security vetting is mandatory for any access.

Tags

Information management