Completing an intelligence report

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

First published 13 January 2026

All staff involved in collecting intelligence should submit an intelligence report (IR) as soon as practicably possible after collection. The IR is used to:

- submit and evaluate information
- manage **dissemination** of intelligence
- protect the source
- act as an **audit trail** of the intelligence

View an example of how an IR could look in **Appendix A**.

Staff who collect intelligence should ensure that the report:

- has the correct GSC marking
- is clear and concise, and does not use abbreviations
- is of value and is understandable without the need to refer to other information sources
- serves a policing purpose (more information in the **Code of Practice on Police Information and Records Management**)

The **IPP introduction to intelligence** (you will need to log in to College Learn) provides practical exercises for completing an IR. The following sections provide information on how to complete an IR.

3×5×2 process

The IR is standardised by the 3×5×2 process, which helps to provide a shared confidence between the police and partner agencies.

- 3 – Source evaluation. The reliability of the source is recorded here (for example, 2 is an untested source).
- 5 – Information or intelligence. How the **information or intelligence assessment** is known to the source . An officer on patrol should grade what they have seen as ‘A’. A report from a member of

the public of something overheard could be ‘C’.
- 2 – Handling codes. The **handling codes** (code P or code C) and how the information or intelligence can be used.

There is more information available in the **handling codes section**.

Person reporting information (source)

When completing an IR, staff should record the name and address of the person providing the information or an existing intelligence source reference (ISR) number.

Report unique reference number

After an IR has been completed, a unique reference number (URN) will be electronically generated by the receiving intelligence unit. If an IR needs to be sanitised, a new IR and URN will be created. When this happens, staff should ensure that the original IR is:

- cross-referenced to the amended report
- stored securely, preventing source details from being revealed

Source evaluation

Source evaluation establishes the credibility of information and informs the proportionality of tactical options if the information is acted on by the police. Staff submitting the intelligence should corroborate how the information is known to the source. They should conduct an evaluation to describe the reliability of the source by using source grading.

1 – Reliable

The ‘reliable’ source evaluation is used when the source – which can include non-human sources, such as closed-circuit television – is believed to be competent and information received is generally reliable. It is important that the two tests of competence and veracity of past intelligence are both met before a source is considered to be reliable.

Where either test is not met, staff submitting the report should record the source as ‘not reliable’ and provide a rationale for this decision.

2 – Untested

The ‘untested’ source evaluation relates to a source that has not provided information to the person receiving it before or has provided information that has not been substantiated. The source may not necessarily be unreliable, but the information provided should be treated with caution.

Staff should try to corroborate the source before acting on the information. This would apply to information when the source cannot be determined – for example, when it originates from **Crimestoppers**.

3 – Not reliable

The ‘not reliable’ source evaluation should be used when there are reasonable grounds to doubt the reliability of the source. Intelligence staff should record the reasons for this decision in the IR risk assessment. Reasons for concern could include authenticity, trustworthiness, competence or motive of the source, or confidence in the technical equipment. Staff should seek corroboration before acting on this information.

Information and intelligence assessment

To ensure that the correct gradings are submitted, the individual who has received the intelligence should complete the initial assessment by asking the source questions about the reliability of the information.

Grade A – known directly to the source

- Refers to information obtained first-hand – for example, through witnessing it.
- Staff should differentiate between what a source witnessed themselves and what a source has been told or has heard from a third party.

Grade B – known indirectly to the source but corroborated

- Refers to information that the source has not witnessed themselves, but the reliability of it can be verified by separate intelligence graded as A.
- This corroboration could come from technical sources, other intelligence, **investigations** or enquiries.

- Staff should ensure that the information presented is independent and not from the same original source.

Grade C – known indirectly to the source

- Applies to information where the source has been told by someone else.
- The source does not have first-hand knowledge of the information, as they did not witness it themselves.

Grade D – not known

- Applies where there is no means of assessing the information.
- This may include information from an anonymous source, or partners such as Crimestoppers.

Grade E – suspected to be false

- Regardless of how the source came upon this information, there is a reason to believe the information provided is false.
- Staff should record the rationale for why it is believed to be false in the IR risk assessment.

Report title

A summary title that gives an overview of the nature of the information recorded in the IR should be provided here.

Information content

Staff should record information that has been provided by the source here. This will include dates, times and locations, as well as a description of what was seen or indirectly known to the source.

In the information content section of the IR, staff should not:

- indicate the nature of the source – human or technical
- reveal the proximity of the source to the information
- include any details that would confirm the identity of the source

This approach should continue throughout the IR process and upon completing the final, sanitised version. This may include details of police officers and staff, within either the source field or the main body of the text.

Separate IRs should be recorded if items of intelligence regarding different matters come from the same source. If there is a risk of a source being compromised following several items of intelligence being disclosed about the same issue, separate IRs can be considered.

The ownership of the risk to the source always remains in the originating organisation. Force leads should ensure that procedures are in place to prevent a source's identity from being revealed.

Handling codes

The following handling codes should be used in an IR to balance the risks associated with sharing intelligence against the greater risk of not sharing it:

- **lawful sharing permitted (code P)**
- **lawful sharing permitted with conditions (code C)**

If handling codes are not adhered to, both the sending and receiving organisation could be held accountable for any consequences.

Lawful sharing permitted (code P)

This handling code allows staff to share intelligence for a policing purpose. There should be local protocols in place and a requirement for a partner agency to receive it.

Further information is available in the:

- **Police information and records management Code of Practice**
- **Information Commissioner's Office data sharing guidance**

Staff should ask the following questions when disseminating code P intelligence:

- are there legal obligations?
- who is asking for it?

- why do they want it?
- what are they going to do with it?

Lawful sharing permitted with conditions (code C)

This handling code permits staff to disseminate intelligence but requires the receiving agency to observe conditions as specified in the IR. Application of this code means that the organisation sending the information has applied specific handling instructions. In this instance, staff should risk assess the information received. An **application for public interest immunity** should be considered if the intelligence is subsequently used in court.

Handling conditions

The following table illustrates the different handling conditions that are placed on intelligence.

Government security classifications	Acquisition		Exploitation		
	Source	Intelligence	Handling	Intelligence unit only	
				Action	Sanitisation
Top secret	1 – Reliable	A – Known directly	P – Lawful sharing permitted	A1 – Covert development	S1 – Delegated authority
Secret	2 – Untested	B – Known indirectly but corroborated	C – Lawful sharing permitted with conditions	A2 – Covert use	S2 – Consult origiator
Official	3 – Not reliable	C – Known indirectly		A3 – Overt use	
		D – Not known			
		E – Suspected to be false			

The receiving force should abide by the handling conditions and should contact the force who shared the information before they conduct any activities outside of these conditions.

Intelligence staff should review IRs with conditions to ensure that wider dissemination can occur as soon as is feasible – for example, when an operation has been concluded or is no longer being pursued.

Intelligence units should use the following five handling conditions when sharing intelligence.

Action conditions (only relevant if handling code C selected)

A1: Covert development

- Intelligence may be combined or corroborated with other intelligence, but action cannot be taken directly.
- Permission needs to be sought from the originator before action is taken on any derived intelligence.

A2: Covert use

- Covert action may be taken on this intelligence. However, the source, technique and any wider investigative effectiveness needs to be protected.
- This intelligence should 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 as specified by the source intelligence owner.

Sanitisation conditions (only relevant if handling code C selected)

Before sharing information, intelligence staff should sanitise the IR by removing material that explicitly or implicitly identifies a source or sensitive law enforcement methodology.

S1: Delegated authority

The originator of the intelligence permits the unsupervised sanitisation of the material 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 report risk assessment

An intelligence report risk assessment should be used by intelligence officers to record risks associated with the dissemination of intelligence held within the IR. The assessment should consider:

- ethical, personal and operational risks in respect of the source, the intelligence content, its use and dissemination
- compliance with a legislative requirement or policing purpose
- the justification for decisions made
- the authority of the person making decisions
- the proportionality, accountability and necessity for disseminating the intelligence
- public interest immunity

Before an IR risk assessment is disseminated, intelligence officers should make sure that:

- the IR risk assessment is not disseminated outside the intelligence unit or sensitive intelligence unit – **handling conditions** should be recorded in the IR
- a review of the IR risk assessment takes place when the report is evaluated for dissemination

Evaluation and quality assurance

When an IR has been submitted within a force, intelligence units should further assess information for:

- risks and duty of care issues
- intelligence value
- accurate and full provenance of the information
- consideration for further research and development
- quality assurance of data standards
- consideration for dissemination and requirements for sanitisation

Amendments and checks

Intelligence units should ensure that any amendment to an IR has an **audit trail**. This is important in the event an IR needs to be **disclosed** for evidential purposes, which could include re-submitting a sanitised IR linked directly to the original report.

The individual who submitted the report should be contacted if further clarity or checks are required.

For more information on IRs, go to the **IPP introduction to intelligence course** (you will need to log in to College Learn).

Tags

APP