Intelligence cycle

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

First published 13 January 2026

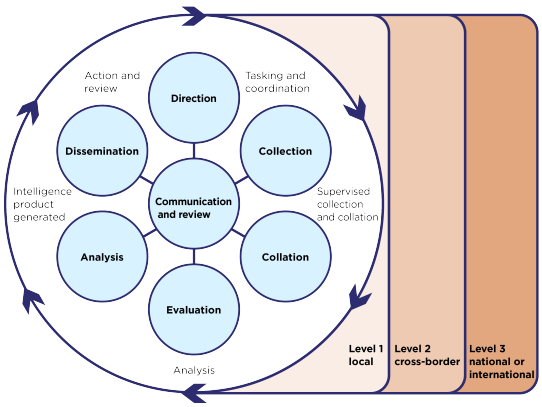
Staff who handle intelligence should follow the processes outlined in the intelligence cycle. This will help forces to assess and understand the scale and nature of threats, and to ensure intelligence is:

- accurate
- adequate
- relevant
- timely
- current

The way that intelligence is handled and received may change depending on where the intelligence cycle starts and the order in which it is completed.

The intelligence cycle consists of:

- **Direction**
- **Collection**
- **Collation**
- **Evaluation**
- **Analysis**
- **Dissemination**



Direction

At the direction stage, the force lead for intelligence should decide the force control strategy (more information available in the control strategy section of the **professional guidance to analysis**). This provides direction and responds to the identified intelligence priorities for the force and local policing area. This strategy is used by intelligence staff to produce intelligence requirements and collection plans.

Control strategies also provide local leadership teams with a framework to prioritise resource decisions.

Intelligence requirements

Intelligence staff should create an intelligence requirement to identify:

- knowledge gaps that are linked to the control strategy
- the different types of information that may be available
- the likelihood of this information having value

An intelligence requirement:

- prioritises information that is needed for a collection plan
- will determine what information is turned into intelligence
- is a dynamic document that focuses on priorities and other key threats identified in the strategic assessment
- is published with the control strategy
- should be communicated to all relevant staff when approved
- needs to be continually reviewed and updated by either the strategic tasking and coordination group (ST&CG) or the tactical tasking and coordination group (TT&CG)
- may need collection strategies to be aligned to it – for example, a covert human intelligence source (CHIS) strategy will influence the activity of the dedicated source unit

There are two different types of intelligence requirements.

- Strategic intelligence requirements outline information that is required to fill gaps in police knowledge (more information available in the strategic intelligence requirement section of the

professional guidance to analysis).
- Tactical intelligence requirements contain information needed to fill in gaps about an investigation or operation (more information available in the tactical intelligence requirement section of the professional guidance to analysis).

If staff receive information that is not linked to the intelligence requirement, this information should still be submitted if it meets a policing purpose. This ensures that relevant information is not overlooked.

Collection

Information can be collected in the following ways:

- routine information gathered by policing responders (for more information, go to routine collection)
- tasked collection
- volunteered information

When information is collected, staff should check whether it has been gathered in accordance with the following requirements, processes and relevant legislation listed.

- Computer Misuse Act 1990
- Criminal Procedure and Investigations Act 1996
- European Convention on Human Rights 1953
- Investigatory Powers Act 2016
- Human Rights Act 1998
- Police, Crime, Sentencing and Courts Act 2022
- Regulation of Investigatory Powers Act 2000
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data protection impact assessment
- Online Safety Act 2023

All staff who collect and share information must do so for a policing purpose only (for more information, go to the **Code of Practice on Police Information and Records Management**). Information that is collected or shared for any other reason could result in a criminal offence.

When staff receive information, they should conduct the following checks when it is validated and recorded and when an **intelligence report** (IR) is completed.

- Whether the information is known to other members of the public or police officers and staff.
- Where the information has come from. The identity of the person providing the information needs to be documented on intelligence systems where known (for more information, go to the **CHIS Code of Practice**).
- How reliable the information is and how it can be shared while suitably protecting the source, if it has been gathered via technical or sensitive means.
- How long the information has been known for.

The checks outlined will assist operational decisions and inform how duty of care is managed. For more information, go to **source evaluation**.

Intelligence collection plan

Intelligence collection plans ensure that the collection phase remains focused, structured and directed. More information is available in the terms of reference (ToR) section in the **professional guidance to analysis**. When intelligence staff create a collection plan, they should make sure that it:

- is current, accurate and updated regularly so that information collection can be properly managed, ensuring that gaps, additional potential sources and possible access difficulties are identified
- contains the necessary information requirements to inform a comprehensive and accurate intelligence picture
- provides justification regarding the proportionality and necessity of the activities that will be used for collecting the information

The content of an intelligence collection plan can vary according to the intelligence requirement or source used. This can include:

- community intelligence, such as neighbourhood watch groups or members of the public

- **open-source research**, such as the results of internet intelligence investigations (III) – more information available in the National Police Chiefs' Council (NPCC) **III Covert Profiles** and **III Overt Profiles**
- forensic materials
- communications intelligence, such as telephone data or social media data
- images
- a **CHIS**
- covert and/or sensitive collection techniques

Intelligence staff should make a record in the collection plan of:

- when sources have been contacted or searched
- deadlines for the return of information
- when information has been received

Intelligence unit managers (you need to log in to College Learn) should oversee the review and implement the collection plans.

Tasked collection

Tasked collection is when information is needed about a specific problem or subject that has been identified in an **intelligence requirement**. Policing responders and intelligence unit staff are usually asked to complete tasked collection.

When staff are tasked to collect information, they can use the following methods and sources:

- proactive activity, including surveillance
- **tasking of a CHIS**
- tasking neighbourhood teams
- interrogating national systems, such as the Police National Computer (PNC) and Police National Database (PND)
- interrogating local force systems
- conducting intelligence interviews
- tasking partners
- **open-source research**, such as III – more information available in the NPCC **III Covert Profiles** and **III Overt Profiles**

Volunteered information

Individuals who provide information to the police do so with an expectation that their identity will be protected. British case law supports this principle (for more information, go to **Swinney and another v Chief Constable of Northumbria [1997] QB 464**).

All staff who obtain information from members of the public need to consider duty of care principles (for more information, go to **Caparo Industries PLC v Dickman [1990] UKHL 2**). For more information, go to the **Information management APP**.

Intelligence staff should conduct a review when an individual has provided information on three separate occasions. This is required to identify whether the person providing the information falls under the **Regualtion of Investingatory Powers Act (RIPA) 2000** definition of a CHIS and requires oversight from a directed surveillance unit.

For more information about the ownership and implementation of this process, go to the **CHIS Code of Practice**.

Corroborating collected information

Intelligence staff should conduct open-source and closed-source research to corroborate **collected information**.

Open-source research

Open-source information is widely available, but may not be accurate, reliable or valid. The main uses of open-source information are to:

- develop an understanding of the locations relevant to a piece of **analysis**
- identify the potential impact of social and demographic changes
- identify external factors that may have an impact on crime, disorder and community concerns
- support and develop **investigations** by indicating lines of enquiry or corroborating other information
- support the development of **subject profiles** and **problem profiles**

The following factors should be considered when using open-source information.

- Access may require the user to register with an account or pay a fee.
- An **audit trail** should be kept and saved in the event the research is used evidentially.
- Security policies may prevent staff from accessing open-source information.
- Compared to **closed sources**, different quality standards apply to open sources. More information is available in the **NPCC III Overt Profiles** (sign-in required).
- If a **directed surveillance authority** is needed, advice should be sought from the local covert authority bureau.
- The content can be removed at any time.
- Information should be corroborated by a different source, rather than relying on open-source information alone. This is known as parallel sourcing.

Staff should consider relevant legislation and force policies when open-source information is being used for intelligence purposes.

Go to **Open source 4** (you need to log in to College Learn) for more information on legislation relating to open-source research.

Internet Protocol (IP) addresses

When intelligence staff access open-source information online, a footprint identifying the IP address is left on the website. A mis-attributable IP address is sometimes required to avoid being identified as the originator of the enquiry. Staff should seek advice from a covert internet investigator and a digital media investigator in these instances.

For more information, go to:

- **NPCC internet intelligence and investigations strategy** (sign-in required)
- **NPCC III Covert Profiles**
- **NPCC III Overt Profiles**
- **Operation Modify: Improving digital thinking** (you will need to log in to College Learn)
- **III investigator learning programme**

Closed-source research

Closed-source data is not widely accessible and has restricted access. It is available from:

- police crime-recording systems

- information available through **information-sharing agreements** (ISAs)
- other police forces
- specialist closed sources – for example, financial intelligence, **counter terrorism policing network**, sensitive intelligence network, **prison intelligence**
- existing intelligence and analytical products (more information available in the section of the **professional guidance to analysis** on other intelligence and analytical products)
- information from partners, including the **National Crime Agency** (NCA), **His Majesty's Revenue and Customs** (HMRC) and the **Home Office Intelligence Directorate**
- organisations that are part of the local **community safety partnership**

A covert internet investigator and a digital media investigator may be required to access some closed-source information.

More information is available in the:

- **NPCC III Covert Profiles**
- **NPCC III Overt Profiles**

Development

The development of collected intelligence should continue throughout prevention, **investigation** and enforcement activity. All methods for developing intelligence should be considered. This can include:

- data research
- communications data analysis
- CHIS tasking and covert deployments
- PND
- **intelligence products**
- communicating probability

Staff who are involved in the collection, analysis and dissemination of intelligence have a responsibility to ensure that a current and accurate intelligence picture is continuously maintained. They are also responsible for communicating this to the appropriate individuals or units.

Collation

Intelligence staff should undertake the collation stage of the process to ensure that intelligence is stored appropriately and is retrievable. Information can be stored and organised using databases, spreadsheets, tables, maps and charts (more information available in the collation table in the **professional guidance to analysis**). These products should then be synthesised, evaluated and interpreted to form the analytical product.

The collation stage should be supervised by a member of staff who is **IPP-trained**. To assist with the collation stage, intelligence staff should refer to the **Information management APP**.

More information on collation is available in the **professional guidance to analysis.**

Evaluation

Effective evaluation ensures that the intelligence is correctly prepared, handled and disseminated.

Intelligence staff should evaluate the collected information to check that it is:

- reliable
- valid
- relevant to the ToR (more information available in the terms of reference section in the **professional guidance to analysis**)
- linked to other information

Before the information is used to support a **collection plan** or an **intelligence product**, the individual submitting the information should evaluate its validity by **completing an IR**. This will help to understand the source or grading of information and the content of it. Information from police staff and officers does not generally need to be evaluated through the IR process and is usually deemed to be reliable.

Analysis

The analysis stage of the intelligence cycle should be carried out by **intelligence analysts** and used to inform decision makers of possible solutions to an issue. This can be achieved by:

- reviewing information to get an accurate picture of the problem
- making informed suggestions on what is known or what might happen

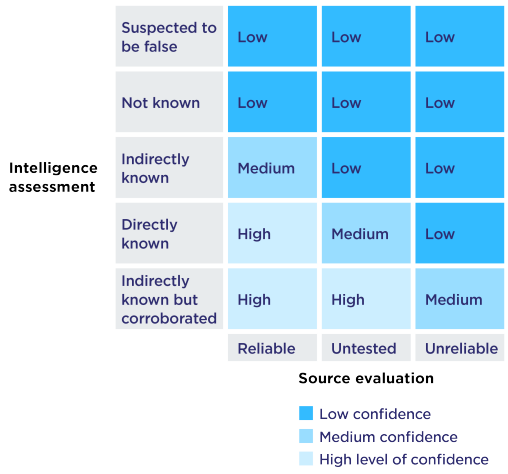
More information is available in the analytical techniques section of the **professional guidance to analysis**.

Dissemination

Intelligence sharing should be proportionate, necessary and carried out in accordance with principles of the following.

- **Computer Misuse Act 1990**
- **Criminal Procedure and Investigations Act 1996**
- **European Convention on Human Rights 1953**
- **Investigatory Powers Act 2016**
- **Human Rights Act 1998**
- **Police, Crime, Sentencing and Courts Act 2022**
- **Regulation of Investigatory Powers Act 2000**
- **Data Protection Act 2018**
- **Data protection impact assessment**

Intelligence should be shared with partners for safeguarding purposes when there is a real and credible risk about individuals or known situations. Intelligence staff should use an audit trail to record whom intelligence has been shared with.



Staff who handle intelligence should use the intelligence confidence matrix to inform decision-making and to support interoperability between agencies or organisations when disseminating

information.

Before intelligence is disseminated, staff should check that:

- the information is up to date
- its collection, analysis and dissemination meets standards set out in:
  - appropriate legislation
  - organisational policies
  - standard operating procedures
  - other relevant frameworks

This is particularly important when handling confidential or sensitive intelligence. When intelligence is disseminated to other forces and partner agencies, staff should abide by the relevant **handling codes and conditions**.

The following guidance and protocols will assist in the dissemination of intelligence to other forces and partner agencies.

- **Charging and case preparation** (disclosure)
- **Data protection** (information sharing and disclosure of information)
- **Information sharing** (common law police disclosure)
- **Freedom of information** (prohibitions on disclosure)
- **Attorney General's guidelines on disclosure**
- **Director of Public Prosecutions' guidance on charging**

Authorisations

Police inspectors or police staff equivalent should develop an **information-sharing agreement** to ensure suitable levels of authorisation for the dissemination of intelligence. The agreement should include any requirements or considerations that should be given in relation to dissemination to non-prosecuting parties, such as educational establishments and healthcare professionals.

Dissemination to non-European Economic Area countries should be authorised by a police inspector or police staff equivalent or above.

Audit trail

Intelligence staff should record an audit trail when intelligence has been disseminated. This should contain information on the:

- recipient
- material disseminated
- purpose of dissemination
- authorisation
- restrictions on the use or further dissemination of the information
- additional IR risk assessment form if appropriate

More information is available in the:

- **Information management APP**
- **IPP Introduction to intelligence** (you will need to log in to College Learn)

National tasking systems

The serious and organised crime tasking system allows intelligence staff to access a set of resources and capabilities in relation to organised crime. These resources are available nationally and their allocation is dependent on the demand that a specific organised crime group (OCG) places on a force or region. More information on serious organised crime tasking systems is available in the **NPCC serious and organised crime local policing framework**.

If information or intelligence shows that an OCG has a criminal impact outside of a police force's area of responsibility, intelligence staff should:

- record the impact on the force's area of responsibility through the central reporting mechanism
- harm-assess that impact (more information is available in the MoRILE section of the **professional guidance to analysis**)
- disseminate all appropriate information or intelligence to the relevant partner or agency for action

Intelligence staff should liaise with their regional organised crime units (ROCUs) who have **ISAs** and memoranda of understanding relating to OCGs. The intelligence staff should ensure that the 'not for dissemination' marking in the serious and organised crime tasking system is used only in exceptional cases.

Communication and review

Intelligence can pass through the intelligence cycle at different stages. It should be continuously reviewed by all staff that handle it to ensure that it is up to date. Intelligence should be reviewed by:

- revisiting earlier stages of the intelligence cycle
- responding to communications from stakeholders
- reviewing intelligence products

Priority levels

Intelligence managers should ensure that the intelligence cycle is aligned. Information and intelligence should flow between the different levels outlined below.

- Level 1: Local – crimes affecting a local policing area.
- Level 2: Regional – where local-level criminality is happening between forces and requires more specialist resources, such as ROCUs.
- Level 3: National or international – serious and organised crime. In most cases, national agencies and organisations such as the **NCA**, **Border Force**, sensitive intelligence units or **Immigration Enforcement** will deal with these issues.

Forces that wish to offer assistance to an international partner should ensure that human rights obligations are met.

For further guidance, go to the:

- **Overseas Security and Justice Association Guidance**
- **Joint International Crime Centre**

Tags

APP