Common process for managing police information

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

First published 23 October 2013 Updated 29 August 2019
Written by College of Policing
5 mins read

Information comes from various sources and is received in different ways. As a result, it may be necessary to link information collected for one policing purpose to information collected elsewhere for a different purpose. Some police information is acknowledged as critical.

Common process at force level

At force level, the following is required.

- Processes to enable information to be linked, and composite records to be maintained.
- Effective **management of police records**.
- A central oversight of all information held within the organisation – this can be facilitated by technology, although even the best IT systems depend on consistent processes being in place and adhered to.
- An **information management strategy (IMS)**.
- **Key roles** to support effective information management.
- Consistent processes to manage information as a corporate resource.
- One business area to link to a record held within another business area. Processes should be managed so that information can be shared where necessary. Consideration should also be given to business areas that contain sensitive information.

Certain public protection matters also need appropriate consideration.

Management of police records

The integrity of police information relies on the information being trusted, acceptable, usable and available. It should be in a format that is accessible and easy to use, whether it is an electronic,

photographic or paper record.

The purpose of records management is to ensure that police information is documented and maintained in such a way that its evidential weight and integrity is not compromised over time. To achieve this, records need to be managed throughout their lifecycle, from creation through to disposal. This process requires records to be audited and maintained so that they remain a useful tool for policing purposes.

Records should be managed in accordance with a records management policy.

For further information, see **Lord Chancellor's (2009) Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000**.

Critical information areas

The **intelligence management** process has a significant bearing on determining critical police information. The development of a national strategic assessment identifies overall risk areas for policing, and contributes to the national community safety plan.

Home Office (2005) Code of Practice on the Management of Police Information acknowledges that there are types of information which are critical to efficient public protection arrangements, described as certain public protection matters. These are a subset of public protection generally and refer to only those offenders who pose the highest possible risk of harm.

Public protection

In this context, public protection refers to offenders who have been convicted of serious sexual or violent offences and who are the subject of extended supervision or registration arrangements. Public protection also includes potentially dangerous people who may not have been convicted of serious offences, but whose behaviour causes significant concern about their risk of serious offending in the future.

Certain public protection matters

For the purpose of information management, certain public protection matters relate to the following.

- Information relating to all offenders who have been managed under multi-agency public protection arrangements (MAPPA).
- Information relating to individuals who have been convicted, acquitted, arrested, questioned, charged or implicated in relation to murder, a serious offence as specified in the **Criminal Justice Act 2003**, or historical offences that would be charged as such if committed today.
- Potentially dangerous people, ie, those who have not been convicted of, or cautioned for, any offence of a sexual or violent nature and who do not fall within any of the MAPPA categories. Their behaviour, however, gives reasonable grounds for believing that there is a real likelihood of them committing an offence or offences likely to cause serious harm.

Information management strategy

The IMS is a high-level document (required by **Home Office (2005) Code of Practice on the Management of Police Information**) which sets out the principles for information management within a force. The strategy is owned by the chief officer and should be available to all staff. It should also be made available to partners and the public. The IMS identifies the information community and defines the processes for managing information within the force and with partners. It allows information to be exploited wherever it is needed within the force, and defines how barriers can be overcome.

The IMS sets out the following.

- Who is responsible for police information held within the force; also known as the data controller.
- The purposes for collecting and holding information.
- Which business areas hold information within the force, and the standards that will apply within those areas.
- The safeguards applied to police information held by the force.
- The relationship between police information held within different business areas.
- Which processes ensure that police information is audited for accuracy and relevance to the policing purposes.
- The controls that are applied to ensure the integrity and security of police information held by the force.
- The training required to support the management of police information.

- The dedicated resources which support the delivery of the IMS and their relationship to other business areas.
- Arrangements for receiving records and monitoring record keeping.
- How the force complies with national and local security policy and standards.

Responsibilities for managing police information

The chief officer:

- has overall responsibility for a force's compliance with **Home Office (2005) Code of Practice on the Management of Police Information**
- owns the IMS and is responsible for ensuring that force policies and processes comply with national guidance
- may wish to appoint someone to oversee all information held by the force (this role would be accountable to the chief officer for the everyday management of police information within the force)

The **Data Protection Act 2018** places a legal obligation on the chief officer, as controller, to comply with the data protection principles, subject to exemptions, in relation to all personal information processed by the force.

All staff must:

- apply the basic principles of effective information management as contained in **Home Office (2005) Code of Practice on the Management of Police Information** and this APP
- apply the **data quality principles** to all police information
- apply the operating rules relevant to the business areas to which they have access
- apply the rules relating to information security
- ensure compliance with all relevant legislation, including the **Human Rights Act 1998**, **Data Protection Act 2018** and **Freedom of Information Act 2000**

Tags

Information management