Information and data management

The legislation behind the governance of the systems.

First published 31 March 2023 Updated 15 May 2024
12 mins read

Information management

Information management is the procedure of collecting, storing, and organising data in a way that allows for efficient retrieval and use. Its purpose is to ensure that the right information is available to the right people at the right time, in order to facilitate decision-making and support the efficient operation of an organisation.

The **Code of Practice on Police Information and Records Management (PIRM) 2023** replaced the Code of Practice on the Management of Police Information 2005 (MoPI). It broadens the applicability of the original MoPI Code beyond records that contain police operational information to include police corporate information.

For the purposes of PNC and LEDS, the operational data that is recorded is also covered by the PIRM Code. Good records management supports good data governance and data protection.

Maintaining integrity and quality assurance of both the systems and the data and the information within are themes which run through both the Code and this guidance.

The ten principles of the Code have been assigned responsibilities or obligations that describe the required good practice for managing and using data contained, accessed or processed in other ways through either PNC or LEDS. Other supporting functions, such as training and securing the data, have been similarly described. Further guidance is contained in College of Policing APP on **Management of police information**.

Review and disposal

Data must only be retained proportionately to the law enforcement purposes and must comply with the fifth data protection principle under Part 3, Chapter 2 of the DPA 2018 (that is, for no longer than is necessary for the purpose for which it is processed).

As part of their information management responsibilities chief officers are required to implement appropriate review and retention procedures and periods. For policing there is:

- specific guidance on deletion of information and records on local systems issued by the NPCC supported by the College of Policing management of police information APP
- guidance issued by Police Scotland and Police Service Northern Ireland (PSNI) for those jurisdictions
- guidance relating to specific material (such as covert, biometric and evidential material)
- a risk-based retention schedule

Disposal of information should be the product of a deliberate and purposive decision rather than a ‘default’ position of non-deletion.

Deletion of records on PNC and LEDS

The review, retention and deletion rules for data on local systems do not apply to the deletion of information and records held on PNC, and by default LEDS. Data held on PNC is currently subject to specific NPCC issued guidance (issued on behalf of the joint controllers) concerning retention of convictions which will extend to LEDS. This guidance is under review during 2024.

Forces should not remove these from PNC or LEDS unless they are incorrect or authorised by the Secretary of State, such as disregarded offences and court orders out of court disposals and other ‘event histories’. This recognises the requirement for policing to hold that criminal history information for policing purposes.

Managing individual rights

For individuals whose personal data may be processed either with or without their consent, there are some legislative protections and rights.

Part 3, Chapter 3 of the DPA 2018 and the UK GDPR provide the following individual rights that must be communicated to data subjects in clear and plain language.

- The right to be informed.
- The right to access.
- The right to rectification.

- The right to erasure or to restrict processing.
- The right to portability (UK GDPR only).
- The right to object (UK GDPR only).
- The right not to be subject to automated decision-making.

The terms of Part 3 of the DPA 2018 and the UK GDPR are not identical. Both provide exemptions and restrictions that can, in some circumstances, be legitimately applied to restrict an individual's rights, but may have different implications. Most of the rights outlined above apply to data collected under Part 3 of the DPA 2018.

Some of the rights only apply under the **UK GDPR**, specifically, the right to object and the right to data portability. These rights will apply to, for example, data collected and processed for safeguarding or immigration purposes.

Further, there are exemptions and restrictions that can, in some circumstances, be legitimately applied to prevent individuals from being granted the rights listed above when considered under law enforcement purpose. In Schedule 2 of the DPA 2018, for example, subject access rights and the rights to rectification, erasure and restriction do not apply to the processing of 'relevant personal data' during a criminal investigation or criminal proceedings. 'Relevant personal data' here means personal data contained in a judicial decision, or in other documents relating to the investigation or proceedings, that are created by – or on behalf of – a court or other judicial authority.

Sensitive data

There are additional provisions in data protection legislation that apply to the management of 'sensitive' personal data (section 35.8 DPA 2018) or 'special category data' (UK GDPR).

In Section 35.8 sensitive processing is defined as:

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual

(c) the processing of data concerning health

(d) the processing of data concerning an individual's sex life or sexual orientation

The UK GDPR definition covers the same data but worded slightly differently.

The legislation requires the controller to have an appropriate policy document in force at the time the processing takes place. Organisations that access PNC and LEDS must be able to demonstrate that such processing is strictly necessary – for example, for the administration of justice or for safeguarding children or individuals at risk.

Criminal offence data is also treated in the same way if the processing organisation is not a 'competent authority' (see **Data protection – definitions and elaboration** for further definition of competent authority) that is, is not an organisation which generally processes data for law enforcement purposes.

Likewise if the organisation is a competent authority processing that data, but for purposes not related to law enforcement. For example, a police force is a 'competent authority' but when processing data about its employees' criminal records for human resources purposes, the force needs to comply with the UK GDPR.

Biometric data

The processing of biometric data constitutes sensitive processing under Part 3 of the DPA 2018, and law enforcement organisations must ensure that they demonstrate that the processing is strictly necessary and satisfies one of the conditions in Schedule 8 of the Act or is based on consent. For example, arrest and detention provides a lawful basis for taking prints and DNA samples.

The Protection of Freedoms Act 2012 (PoFA) curtailed the power to retain biometric data from suspects who are not charged or convicted of any offence. The PoFA also reduced the length of time for which data can be retained, with only the data of those convicted of the most serious offences being subject to 'indefinite' retention.

Freedom of information and public access requests

Freedom of information requests

The **Freedom of Information Act 2000** (FOIA) provides any person, anywhere in the world, the right to access information held by public authorities, subject to certain exemptions.

All police forces and public organisations using LEDS are separate public authorities subject to this Act, as are the College of Policing and the Home Office. Guidance from the ICO is available to help organisations meet those responsibilities.

The FOIA interfaces with the DPA 2018. APP on information management provides specific guidance on handling such requests in accordance with local policies and procedures.

Subject access requests

Individuals may exercise the legal right to access information held about them by making a subject access request (SAR). This can be made by phone, in person, or in writing.

Requests for information held about an individual may require identity verification. Historically, for policing, ACRO Criminal Records Office has processed data SARs relating to PNC on behalf of most UK police forces by agreement. However, this is primarily an organisational responsibility.

There is specific guidance issued by the NPCC to manage an application for record deletion made by an individual whose data may be held on the national systems. This is known as the NPCC Record Deletion Process (RDP). This policy is under review as of February 2024.

NLEDP and ACRO are also in discussion regarding a centralised Data Subject Access Requests process. This would ensure that there is a readily accessible process for individuals to exercise their rights in respect of data held through LEDS and would support organisations in meeting their legal responsibilities in responding to requests. This will be realised within a new LEDS product ‘Person’ but development of this product is still in early stages as of February 2024.

Accurate data, coupled with robust and reliable processes and procedures by which to manage SARs, will result in both a time and financial benefit to the organisation. The ICO can take, and has taken, enforcement action against organisations (including policing), which includes financial penalties for not adhering to strict timelines on response to SARs.

Disclosure and the Rehabilitation of Offenders Act 1974

Although that information may be retained on the central policing records, cautions, reprimands and warnings and some convictions are deemed to have become ‘spent’ after a certain period under the **Rehabilitation of Offenders Act 1974.** Once a record becomes spent, it does not usually need to be declared to employers or voluntary organisations.

When a person applies for a so-called ‘excepted position’, they may be required to provide details of their criminal record, both spent and unspent, by way of a standard or enhanced criminal records check from the Disclosure and Barring Service (DBS), Disclosure Scotland or AccessNI. There are certain exceptions set out in the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (as amended). This is in recognition that there are certain activities for which fuller disclosure of a person’s criminal record history is relevant, for example, work with children or vulnerable adults, or roles in certain licensed occupations or positions of trust.

The government amended the **filtering guidance** that explain what is automatically disclosed in November 2020. Further revised guidance has recently been issued on what locally held information should be included on an enhanced DBS certificate. The decision as to whether local police information should be disclosed on a certificate rests with chief officers in forces. Recognising the sensitivity of disclosing such information, they must have regard to **statutory disclosure guidance** issued by the Secretary of State.

Data quality

Improving and maintaining data quality is one of the significant themes that runs through the Code and this guidance. The LEDS programme is reviewing the quality of data that comes into LEDS from PNC. The value that data brings to policing, law enforcement and other users is dependent on the quality of that data as held on the system. It is a clear expectation that all user organisations will ensure that data that is inputted or uploaded to PNC and/or LEDS is of the highest possible quality.

The National Police Data Board (NPDB) and National Police Data Office (NPDO) will support all work undertaken to improve data quality in policing. The NPDB brings together subject matter experts in relation to data quality, records management, data protection and data sharing, the aim being to create a consistent framework for the management and use of data. Data quality forms a critical part of the development of LEDS through to sustainment and business as usual. There is a dedicated team that will work with policing to ensure that the following activities take place.

- Creating a data prioritisation plan – which will ensure the programme focuses on the data which matters most to policing.
- Defining standards – clarity on expectations locally and nationally.
- Addressing root causes of poor data – understanding the root causes of poor data and ensuring that we cascade this learning.
- Support and resources – providing guidance to support policing in maintaining high quality data.
- Data quality tooling – exploring what technical solutions (including AI and robotics) could be deployed to support the cleansing of data.

The LEDs programme has initiated a Data Quality Service (DQS) as one of the LEDS support services which works across the programme. A policing-led LEDS Data Governance Board (LDGB), which includes the LEDS Programme Portfolio Data Lead and representatives from the DQS, will work together to support high quality through:

- working with policing to support the implementation of minimum data quality standards across local systems to ensure that national data sets meet operational requirements
- applying a Data Quality Strategy, a framework against which performance will be monitored and managed
- working with stakeholders to embed core concepts of quality within policing data literacy curriculum currently in development
- providing clarity on what is expected in terms of data quality and defining what does good look like

DQS will work across LEDS product teams to establish the data demands and ensure they’re met, analyse data quality and investigate any concerns raised about the data that is either being uploaded or created within LEDS.

Checklist for data controllers

The following checklist must be considered by data controllers when executing their obligation to comply with the principles of the Code.

- All policing data shared with national systems must comply with national minimum data standards. For example, POLE (Person, Object, Location, Event) standards are still considered as good practice in standardising data creation.
- Any errors that are identified will be rectified as soon as practicable.

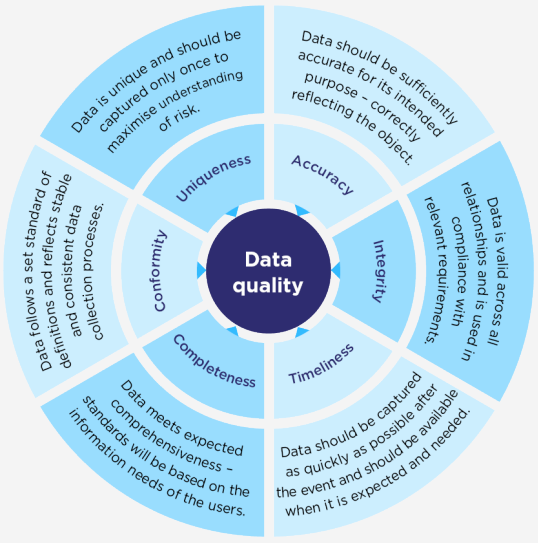
- All staff within the organisation understand the importance of high data quality and have access to the necessary tools and support to achieve this.
- Appropriate training is provided to ensure that the highest levels of data literacy are achieved and maintained.
- There is a formal, local governance process for the management of data quality with clear responsibilities.

Data quality standards

Six data-quality dimensions have been identified by the **Data Management Association UK (DAMA UK)** and are embedded in the **Government Data Quality Framework** as the recommended core data-quality standards for the public sector and are outlined below.

These are:

- accuracy
- integrity
- timeliness
- completeness
- conformity
- uniqueness



These, together with the national minimum POLE standards, serve as guidance to help forces and other inputting organisations identify how to improve the quality of the data being transferred to the national systems, or directly inputted.

The quality of that data will be assessed to ensure that adherence to the required standard and organisations will be expected to comply as far as is practicable. More detailed guidance will be produced to enable users to input data correctly, and for managers and reviewers to identify how to apply quality controls.

Tags

Information management