Accountability, compliance and malpractice

How the Code of Practice and guidance will be used to hold chief officers and users to account.

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

Accountability

The Code, together with this guidance, may be considered in a court of law and referenced in disciplinary proceedings where it is relevant to do so. Breach of specific legal requirements, such as compliance with the DPA 2018 or the deletion of DNA profiles and fingerprints under the Police and Criminal Evidence Act 1984, as amended by the Protection of Freedoms Act (PoFA) 2012, should be treated in accordance with the relevant legislation.

The Code and guidance will be considered by those bodies who may seek to hold users to account for data management practice in a law enforcement or safeguarding context.

The ICO

The Information Commissioner's Office (ICO) is the independent regulatory body dealing with data protection legislation.

The role of the Commissioner is:

> *...to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.*

The ICO covers a number of pieces of legislation including the **Data Protection Act 2018**, the UK **General Data Protection Regulation** and the **Freedom of Information Act 2000**.

Part of their role is to:

- provide guidance information
- respond to consultations (such as the consultation on the Code)
- advise organisations on compliance

- take action to ensure organisations meet their information rights obligations by investigating concerns or responding to complaints

The ICO will respond on receipt of a formal complaint or to a self-referral, as occurs in the event of any breach of data privacy that is likely to result in a risk to the rights and freedoms of individuals.

The ICO also has power to undertake consensual and compulsory audits across the public and private sector.

These audits allow them to:

- assess the processing of personal information
- provide practical advice and recommendations to improve the way organisations deal with information rights issues

HMICFRS

His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) independently assesses the effectiveness and efficiency of police forces and fire & rescue services – in the public interest.

HMICFRS:

> *...oversees, inspects and reports upon the efficiency and effectiveness of all Home Office police forces, as well as other forces and agencies by invitation.*

HMICFRS may use **the Code**, together with this document and any associated performance standards, to hold organisations who access PNC or LEDS systems to account for their data management practice. Compliance with the Code may now be considered within general inspection of police forces, although there are no immediate plans for any specific thematic reviews.

As a new Code of Practice there has been a one-year-lead-in period for forces to assess their levels of compliance and understand where they may need to change processes or address deficits. This has been supported by the NPCC and NLEDP as part of the transition from PNC to LEDS. A **compliance framework tool** (available on Knowledge Hub for members of the LEDS group) has been developed to support policing and other users organisations to make that

assessment and evidence their compliance. For the purposes of general inspection HMICFRS will consider a completed self-assessment as evidence towards Code compliance.

Through the written access agreements, HMICFRS will also have powers to inspect other organisations that have access to PNC or LEDS.

Within these written access agreements will be an agreement that they will:

- adhere to national minimum data standards
- apply industry standard data quality dimensions
- comply with processes such as those identified by internal and external audit
- use specific performance metrics for monitoring

Other bodies

The Biometrics Commissioner and the Independent Office for Police Conduct are likely have an interest in how the Code is applied.

As LEDS develops, further consideration may be given to additional independent oversight arrangements. This will address key issues such as consistency in applying the Code principles by LEDS user organisations.

Audit and performance monitoring

Principle 9 of the Code is Accountability for and auditing of data access and usage. The DPA 2018 and the UK GDPR emphasise organisational accountability when processing any information that falls within the definition of personal data, and that includes monitoring compliance with data protection requirements.

An audit is a pro-active systematic, independent examination of organisational processes, systems and data to determine whether activities involving the processing, use and sharing of the data are being carried out in accordance with the UK GDPR, DPA 2018 and other expected legal and performance standards.

Audit for PNC

Audit for PNC has traditionally taken the form of user or compliance audit, managed through data protection compliance structures. This means monitoring of end user activity to:

- ensure compliance with regulatory standards and legislation
- identify, investigate, respond to and deter wrongdoing

This is distinct from cyber security audit and quality audit. Cyber security audit monitors external interference. You can find more information in the **Guidance on Compliance Audit**.

User audit is usually carried out by local auditors in forces. In PNC, auditors can check records of transactions at a certain date and time and see which users were accessing the system. They can also check transactions against a nominated user and see what they were looking for.

This might involve regular reviews of recent user activity (as dip sampling) or more specific reviewing activity by person, time, or type of transaction. Audit practice across forces is variable and it is reported that the number of dedicated trained auditors may have dwindled. Forces may make use of commercial products such as PNC Guard which automates part of the audit process.

Audit for LEDS

Audit for LEDS will also facilitate user audit. Audit is being developed as a support service product for LEDS. New functionality will enable auditors to have a specific audit access which is a more layered access than is currently provided by PNC.

In LEDS local auditors can still check records of transactions at a certain date and time or against a nominated user but LEDS audit search removes limits currently in place on the number of audit transactions returned. This will speed up presentation of evidence when any internal investigations or disciplinary actions are underway. Other functionality under development will allow an auditor direct access to data logs without requesting them from Enterprise Services.

LEDS Audit Product seeks to deliver:

- an evidentially sound storage and retrieval mechanism
- a timely capture of audit
- a timely return of audit data
- end to end traceability across the product and any interfaces

- controlled access for appropriately authorised users
- the ability to audit across the LEDS Products from a single point of access
- an easy to use user interface to reduce operational risk, with the least possible training burden to support the roll out of the audit product in support of the wider product set

LEDS has a National Auditor who will set the guidance for LEDS audit practice.

User malpractice

The Code, underpinned by this guidance, may be considered in a court of law and referenced in disciplinary proceedings where it is relevant to do so. Professional Standards Departments in forces respond to public complaints, internal misconduct reports and intelligence concerning corrupt activity by individual users. They will carry out checks of PNC and LEDS through:

- investigation or clarification – seeking to understanding wider user activity context or intent in a user's PNC activity
- reporting – downloading and sharing data for prosecution and compliance purposes

It is illegal under the Computer Misuse Act 1990 to gain access to a computer without permission (officially known as 'unauthorised access to a computer'). A user who gains access to data unlawfully may face a penalty of up to two years in prison and a £5,000 fine.

If a user gains access to PNC or LEDS without permission in order to steal data or take part in another crime, such as using that data to commit fraud or collaborate with organised crime, they may face a sentence of up to 10 years in prison and/or receive an unlimited fine. The extent of the punishment depends on the severity of the individual case.

Reporting complaints

Concerned parties or individuals whose data may be contained within PNC or LEDS who believe that there may be evidence of breach of the Code, should report those concerns to the relevant police force or the identified user organisation.

This does not supersede the role of the ICO in dealing with concerns raised by members of the public about how personal information has been handled within either PNC or LEDS.

Complaints about functionality of systems

Complaints that may seem to be directed at the general functionality of the systems (rather than the processing of any particular data) should be directed to the Home Office, as technical system manager and administrator.

Internal complaints

For internal complaints, national arrangements are being set up as part of the work on sustainment for the Code to protect those who express concerns about the misuse of data obtained from either PNC or LEDS.

Chief officers are expected to comply with these national arrangements, alongside their statutory obligations in relation to whistleblowing. The existence of the local whistleblowing arrangements will be part of the HMICFRS inspection regime.

Tags

Information management