Information Audit Procedure

This document is part of North Yorkshire Police policy to which all Chief Constable personnel and the functions provided by the Deputy Mayor for Policing as part of the York & North Yorkshire Combined Authority are required to adhere.

Procedure Statement

The Data Protection Act (DPA) 2018 and General Data Protection Regulation (GDPR) 2016, as applied in the UK, places a primary legal obligation on the Chief Officer, as Data Controller, to comply with the Data Protection principles, in relation to all personal information controlled or processed by North Yorkshire Police (NYP) and must be able to demonstrate compliance with these principles.
Failure to record information correctly can prevent forces from being able to adequately manage risk to the public, create potential misuse of resources and not meet national and local policing objectives.

Failure to record information correctly can cause damage and distress to individuals (i.e. data subjects), incur financial penalties, embarrassment and adverse publicity in the media.
Failure to review and retain information appropriately may constitute a breach of legislation and ultimately undermine public confidence in the police service.
The Management of Police Information (MoPI) Code of Practice 2005 requires compliance against all business areas.

His Majesty's Inspectors of Constabulary and Fire and Rescue Services (HMICFRS) will monitor police forces compliance with this Code, associated guidance and standards.

Overarching Policies:
Data Protection Policy
Records Management Policy

Procedures:
Data Procedure
Collection & Recording of Police Information (Niche RMS) Procedure
Review, Retention and Disposal of Information Procedure
National Crime Recording Standard Procedure
National Standard for Incident Recording Procedure
Police National Computer (PNC) Procedure
Police National Database (PND) Procedure

Other Documents:
NPCC Data Protection Manual of Guidance (Available on NPCC Knowledge hub)
Information Asset Owner Handbook
Information Management section of the Authorised Professional Practice (the Management of Police Information Code of Practice and Guidance)
Home Office Data Quality Audit Manual 2018

PNC Code of Practice
PND Code of Practice

Process

There are three forms of auditing that are required to be carried out by forces under the DPA and MoPI:

- Transactional Audits
- Compliance Audits
- Data Audits

Transactional Audits

Transactional audits are regular audits carried out on Force systems to ensure that systems are not being misused. There are a number of Force systems that require transactional audits to be carried out daily to comply with the Manual of Practice. As a minimum the force systems include:

- Police National Computer (PNC)
- Police National Database (PND)

The following areas should be considered as part of a transactional audit:

- transaction field inputs should be examined for quality
- sufficient details should be obtained to trace the inquiry back to the originator
- legitimacy of the check should be confirmed with the originator or by checking documentation
- any errors should be categorised and noted. The collation of the results will enable trends to be identified and remedied
- the number of transactional checks is in proportion to the total number of transactions carried out

The HMICFRS do carry out audits on this function and do request that the following documentation is retained as a minimum:

- annual/strategic audit plans including the supporting risk analysis
- audit plan and audit control sheets
- schedules showing summary detail of audit/monitoring work carried out
- detailed working papers supporting audit conclusions.
- copies of audit reports
- executive board responses to audit report

Compliance Audits

A Compliance Audit is a form of Internal Audit and provides:

- an independent view of whether the supervision and monitoring practices in place are adequate to ensure a high standard of good data quality is being maintained
- an independent view of whether internal controls such as policies and procedures are adequately managing the risk arising from poor information management practices
- identification of specific information which is not held or processed in accordance with Data Protection Principles
- a mechanism to make the Senior Information Risk Owner (SIRO) and business owners aware of the risks arising from poor information management.

A Compliance Audit is carried out to monitor compliance with the Principles of the Data Protection Act 2018, the UK GDPR and the Statutory Code of Practice for the Management of Police Information 2005, forces are required to undertake a programme of Data Protection Compliance Audits.
Compliance audits are structured in the following ways:

- On a bi-annual basis, Information Asset Owners (IAOs), supported by their Information Guardians, will complete an assurance statement for each of their assets. This audits compliance with the data protection principles and audits risk around the confidentiality, integrity and availability of information assets, identifying risk and documenting mitigation put in place – as referenced within the IAO Handbook
- The Data Protection Officer (DPO) reports exceptions and good practice identified in these assurance statements to the SIRO and the Information Assurance Board (IAB)
- Bi-annually (during the years where the above assurance statements are not being completed) IAOs will review the information asset register, using the mini checklist, to ensure all assets are identified and mapped, and all existing dataflow maps have been reviewed for accuracy, in addition to ad-hoc identification of new assets
- All of the above are documented in the IAO Handbook
- The Compliance Team within Information management have an audit programme to dip sample compliance with information security, records management and data protection policies and procedures, to also identify risk. The frequency and volume of dip sampling compliance will be appropriate to the level of risk identified. This audit programme shall be centered around internal information assets and physical locations / departments. External third party (data processors) will also be audited for compliance with security controls and compliance with data protection principles. Non-compliance and risk will be reported to the IAO and SIRO where appropriate.

Data Audits

Data Audits are carried out on the information inputted into force systems, there are two separate processes to data audits:

- Monitoring
- Auditing

Definition of Monitoring
The day to day examination of procedures, data quality, minimum standards and compliance with the objective of ensuring data is entered correctly at the outset, identifying misuse, or errors so that corrective action may be taken.
Monitoring is the responsibility of Line Managers and should be conducted on an ongoing, 'business as usual'.

Definition of Auditing
An examination of specific procedures and data, with the objective of measuring and monitoring the effectiveness of the supervision, by recording incidents of inappropriate access and/or errors.
Auditing is conducted by an independent unit/person internal to the organisation and is a rolling programme of regular inspection process.

Audit Process

The purpose of an audit is to check that the organisation is operating in accordance with its documented policies, code of practice, guidelines and procedures. Audits also give an independent view of data quality and identify whether internal controls such as policies and procedures are adequately managing any risks.
The purpose of each audit is to:

- collect objective evidence about the status of MoPI within the organisation so that a factual, informed judgement can be made about its adequacy and effectiveness
- the auditor must take samples from the selected area and check for implementation and effectiveness of management of police information to arrive at the factual informed judgement
- improve future processes of collecting, recording, evaluating, reviewing or deleting information
- reduce risk to misuse of systems and processes

Various methods of conducting audits are undertaken and are completed by internal departments/teams as well as external parties, as part of NYP's Internal Audit controls.
Audits are prioritised based on risk and are planned in advance. Documents such as policies, procedures, guidelines, previous audit reports (if available), copies of regular data quality checks can be obtained along with any independent audit reports prior to commencement of the audit. Audits can include conducting interviews, focus group discussions and data/information sampling.
The results of any audits will be presented to the most appropriate level within the governance structure which can include the Independent Audit Committee and any actions/recommendations completed accordingly.

Responsibilities

Senior Information Risk Owner (SIRO) and Information Assurance Board

- Approve Audit Schedule
- Approve Audit Report and Recommendations

Information Asset Owners (IAOs)

- Conduct bi-annual assurances statements for each information asset
- Conduct bi-annual and ad-hoc review of information asset register and dataflow maps

Compliance Team within Information Management

- Compile exception report for the SIRO and IAB following assurance statement process
- Audit / dip sample internal and external stakeholders for compliance with information security, records management and data protection policies and procedures.

Auditor

- Complete Audit Risk Assessments
- Complete Audit Schedule
- Complete Data Audits in accordance with Audit Schedule
- Complete Audit Report with recommendations

Line Manager(s)

- Meet to discuss Audit Plan
- Forward any documentation to Auditor
- Provide access to Officers/Staff throughout audit
- Review first draft of the Audit Report and its recommendations

Operational Officers/Police Staff

- Be available to answer questions by the Auditor

Definition of Special Terms
IAO – Information Asset Owner
SIRO – Senior Information Risk Owner
MoPI – Management of Police Information