



Data Procedure

This procedure 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

Data is the information that flows through the organisation and is key to making the right decisions both legislatively and ethically at every level of the organisation in a way that is transparent, scalable, explainable and useable to both individuals, the organisation and the public we serve.

The Data culture (leadership, insight and decision making) of an organisation is underpinned by data quality which is the why, where, how, who, and when data and information is recorded, analysed and presented that enables the legislative compliance, accuracy, system, gaps, corrections, management and ownership of data to be effectively controlled in order to discharge the activities that define policing at all levels of the organisation.

This procedure sets out responsibilities to assist NYP to achieve, maintain and improve the use of data that is held across the organisation.

Overarching Policies:

Records Management

Procedures:

Data Protection

Data Protection - Subject Access

Freedom of Information

Management and Submission of Intelligence Information

Personal Data – the right to rectification and the right to erasure

Information Security

Information Audit

Process

Data culture starts at the (very) top with leaders setting the expectations that decisions must be anchored in data and that this is normal, not novel, or exceptional. This will be expressed through nationally mandated documents like the Force Management Statement, Internal process like the service plans and/or change programmes and also through a consistent, transparent leadership approach that generates trust in the data process. That ultimately enhances service to communities as set out in the

police and crime plan. In delivering this Leaders will set the performance metrics that support the cultural approach of the organisation and are clear in their expectations of Officers and staff in achieving appropriate performance goals that drive organisational outcomes. This is supported through the Business Insight Team whose role it is to support the organisation in achieving those goals.

To drive **Insight** from data requires trust, accessibility and clarity so it is incumbent on the organisation to make it available in a user friendly format, Identify and rectify any issues early , and to explain any constraints to the data (data modelling isn't about absolute certainty but around providing good quality estimates framed by measures of uncertainty). Finally, insight needs to be driven by effective questioning which will be delivered through a mix of commissioning process underpinned with a problem statement approach when questions are complex or difficult to describe.

Finally, data is nothing unless it can drive informed ethical **decision making**. It must be flexible to meet the needs across all levels of the organisation and the statutory bodies that NYP have to report into. To achieve this data analytics needs to be tailored to meet local need, using new ideas and approaches to solve problems, be transparent in the analytical choices being made and effectively underpinned with clear and accountable data sources that are validated by organisation.

Achieving a good data culture is the responsibility of every person in the organisation and must be underpinned by development a data competent workforce that drives up data quality.

Data Quality is defined when the data is considered fit for its intended purpose in; driving activity with a policing purpose, decision making and planning. As such data is a valuable organisational asset that can inform, enrich and enhance policing. Everyone has a responsibility for the data of the organisation in that it is necessary at both a practitioner level to enable an individual to undertake their duties effectively and also at an organisational level to enable North Yorkshire Police to discharge its collective duties effectively. Both of these are equally important because reliable, accurate and complete information is fundamental to achieving effective service and also drive compliance to legislation such as the Data Protection Act 2018, General Data Protection Regulations (GDPR) and the Code of Practice for the Management of Police Information (MoPI).

Data supports informed and effective ethical decision making, future planning, improves customer service, enables effective discharge of statutory duties to the Home Office and HMICFRS, helps to achieve and maintain public confidence and assists in the investigation and detection of offences.

This procedure has therefore been subdivided into eight sections which describes the practitioner, management and corporate approach and responsibility to data and information.

1. **Data compliance** is the responsibility to ensure that systems are updated when required in the correct way to ensure consistency in recording and completeness that meets legislative and/or organisational compliance requirements:

***A Practitioner** is responsible for ensuring that the information is captured once and close to point of when the information was obtained, that it is sufficient for the task required, clear and understandable to others, is in the correct form, field or where directed the agreed wording is used. The practitioner should ensure that the data/information is complete and correctly located on the system to both fulfil its purpose and enable dip sampling, review and data extraction.*

The SMT is responsible for ensuring that the practitioner has the right skills, access, and knowledge of the systems to input data and information into the correct field, forms or wording as described by the organisation.

System owners and administrators are responsible for ensuring that any change or update to systems are communicated to those affected by the change, in relation to where and how data needs to be recorded.

Information Management are accountable for the overall process of ensuring data compliance on behalf of the organisation.

2. **Data Accuracy** is how information is recorded on systems that minimises error and where necessary ensures data uniqueness on systems. Inaccuracies can lead to security incidents and personal data breaches which could carry reputational damage and financial penalties, as well as other enforcement actions from the regulator.

A Practitioner is responsible for ensuring that their data/ information when inputted is spelt or formatted correctly, is factual, meets or aligns to any standard recording definitions put into place by the organisation, and any other national standards and/or legislation.

The SMT is responsible for ensuring that through supervision and effective review that the data and information is accurate, necessary and proportionate, shows a clear rationale for decision making, and opinion is clearly distinguished from fact.

3. **Data systems** are the key structures by which data is ingested, stored and presented for analytical analysis and is fundamental in the delivery of analytical data products. It is critical to data audit, by being able through established data schematics demonstrate the impact of system change.

The SMT is responsible for prioritising data quality when developing and implementing new processes, new systems and/or major system upgrades to ensure that any new data captured is compliant with existing organisation data models enabling data to be extracted and joined to other data sources.

Portfolio Programme Management Office is responsible for engaging with all appropriate stakeholders to ensure that all data considerations, (requirement, compatibility, structure, integration to other systems, organisation and operational needs) are fully investigated.

System owners and administrators are responsible for ensuring that any change or update to systems is tested to ensure that data ingested and then subsequently presented for analysis correlates and is correct.

enableNY(ICT) is responsible for providing the technical advice and expertise to system owners and administrators and support the implementation of any technical fixes or investigations that are ongoing with the system supplier.

Business Insight is responsible for advising and supporting any data testing related to system updates or new systems to help ensure that ongoing data requirements are maintained

4. **Data gaps** are where additional data requirements have been identified to capture information on a repeated basis which sits outside of core systems (A core system as a proprietary system being used for the purpose for which it was designed).

All Practitioners are responsible for ensuring that any information that needs to be captured on a repeated basis which does not sit on a core system is captured in a way that enables the organisation to have oversight of that data. Excel or word is not considered a suitable system for recording this type of data. Where that data is of a personal or restricted nature additional considerations including discussion via Supervision, with Business Insight and PSIU should be considered

The SMT is responsible for ensuring that any data or information that sits within their remit and is not recorded onto core systems is recorded in a manner which is compliant to DPA/GDPR and enables both local and organisational oversight of that information subject to the controls required over the data.

Business Insight is responsible for supporting all organisational teams in the most effective and organisationally compliant manner of collecting and recording information that sits outside core systems.

5. **Data correction** is acknowledging that in any data system, errors will occur and that there is an effective corrective mechanism in place.

A Practitioner (where permission levels and/or training allow) is responsible, when it is identified that data accuracy or compliance has not been followed, to amend the data accordingly either by direct input or ensure that the appropriate function is notified to carry out the amendment on their behalf. Where it is identified that there is an inaccuracy on a record which may also be replicated on a paper record, every attempt where feasible to correct the paper record in addition to the electronic record should be made.

The SMT is responsible for the ownership of data corrections and ensure that they have processes in place to drive data quality improvements including identifying and rectifying skills or knowledge gaps in practitioners. This should include roles and individuals responsible for data corrections that are competent to carry out the activities. Permission to amend, merge and/or delete records created in recording systems should be restricted to specific roles.

Business Insight is responsible for identifying trends and patterns in data that are linked to either system issues or individual data issues and notify respective system administrators and HoF. Significant errors (for example those that might impact on operational decision making or affect national data submissions) will be subject to an internal BI review process prior to notification and managed through Risk and Assurance board.

System owner and administrators are responsible for amendments of system errors and working with ICT/System suppliers to ensure solutions to prevent subsequent data inaccuracies are put into place and technical fixes are introduced so that errors are amended for future data input and back record converted.

6. **Master data management (MDM)** is the core process used to manage, centralize, organize, categorize, localize, synchronize, remove and enrich master data according to the business rules and operational strategies of the force.

enableNY (ICT) will manage the data structures in order to ensure that the data is organised and categorised correctly with access rights and data synchronisation protocols, that gives the organisation confidence in delivering against the operational strategies set.

Business Insight will ensure any data analytical products are compliant to data management rules and that access is restricted to the appropriate level, data is updated (against agreed parameters), the use of data is minimised to what is necessary and is designed around the operational strategies of the force.

Systems owners and administrators are responsible, when appropriate, to receive and review requests for corrective activity and merging. Carry out updates, merging, and deletion as appropriate and in line with local and national standards. Provide assistance with technical solutions to improve the DQ of information recorded.

Information Management is responsible for ensuring compliance across the organisation to master data management process that is underpinned by the rights expressed through legislation (MOPI, GDPR, DPA).

7. **Data Analytics** is the presentation of data and information designed for the end user that will more effectively inform decision making.

Practitioner: is responsible for using data analytical products and identifying amendments, improvements or additions that will facilitate more effective decision making at a local level.

SMT is responsible for driving informed questioning and describing the needs of the organisation through a problem statement approach that will enable more effective understanding and delivery of the right analytical products that improve decision making.

Business Insight is responsible for all organisational data analytical products on behalf of national and local clients through a commissioned service approach that meets the needs of the organisation and are compliant to GDPR and DPA.

enableNY (ICT) is responsible for supporting the acquisition, development, organisation and presentation of core and nonstandard data in a format suitable for analysis.

8. **Data legitimacy** is the overall combined impact of data quality and culture on the organisation's reputation and the impact of public confidence, inspectorate confidence and governmental confidence in the organisation as a whole.

All officers and staff have a responsibility to uphold the data standards of the organisation, its reputation and confidence in the services it provides through ensuring that the data and information it holds is accurate, ethical, legitimate and proportionate.

Definition of Special Terms

NYP North Yorkshire Police
MoPI Management of Police Information
GDPR General Data protection regulations

DPA Data Protection Act