

**PROCEDURE**

<b>Title:</b>	<b>Data Quality</b>	
Practice / Business Area:	Digital Services Division	
Department Responsible:	Data Quality and Audit	
First Published:	16/10/2013	
Last Reviewed:	23/12/2019	
Next Review Due:	December 2021	This document applies to employees of the:
Version Number:	08	Chief Constable

**SOUTH WALES POLICE PROCEDURE OBJECTIVE:**

To improve the quality of data within our policing systems enhancing decision making, increasing performance and reducing risk to victims and witnesses of crime.

**GUIDANCE:**

This guidance and procedure is aligned to the SEWNIC Data Quality Standards which clearly sets out the quality standards expected and required from all inputters of information specifically for Niche RMS. It establishes how the Force, together with its staff and partners, will focus its energy on improving and maintaining data quality.

All Policing Data and information must recognise the MOPI Guidance which draws upon Principles 3 and 4 of the Data Protection Act. It stipulates that all police information must conform to the following data quality principles:

All data must be:

- Accurate
- Adequate
- Relevant
- Timely

This will ensure data and information is fit for purpose. It is the responsibility of all Officers and Staff who input data to ensure compliance and MUST adhere with ALL the standards that are set out in the minimum standards document.

All staff will make themselves familiar with the minimum standards in section 5 of SEWNIC Data Quality Standards. It is the responsibility of every member of staff to accept ownership for any data used and input into all Force systems, and to make themselves aware of the organisational requirements with regard to data accuracy and compliance with MoPI standards.

It will be the role of Managers and Supervisors to ensure all staff comply with the minimum standards in section 5 of SEWNIC Data Quality Standards. A list of all staff that are responsible for inputting poor data will be available to managers and staff for corrective action.

SEWNIC Data Quality Standards covering Niche RMS apply to both Gwent and South Wales Police. The Data Quality Team is responsible for the monitoring of these standards and identifying users who create erroneous data within the core systems.

**PROCEDURE:**

All Policing Data and information must recognise the MOPI Guidance which draws upon Principles 3 and 4 of the Data Protection Act. It stipulates that all police information must conform to the following data quality principles:

**Data MUST be Accurate** - care must be taken when recording information and, where appropriate, the source of the information must also be recorded. If there is any doubt over the authenticity of the information clarification must be sought from the source. Inaccurate information must be corrected as soon as possible. In ensuring accuracy it is important NOT to delete historic information that may be significant (such as details of previous addresses).

**Data MUST be Adequate** - recorded information must be accurate and sufficient for the policing purpose in which it is processed. The nature of the event will determine the information that is relevant (e.g. clearly more information will be necessary from a witness to a fatal incident than a minor road traffic incident). All recorded information must be easily understood by others.

**Data MUST be Relevant** - information recorded must be relevant to the policing purpose. Opinions need to be clearly distinguished from fact.

**Data MUST be Timely** - information must be promptly recorded into the relevant business area in accordance with the agreed timescales.

Officers and staff failing to comply with the standards expected and required of them are identifiable through Business Intelligence query reports. These Business Intelligence reports will assist managers and supervisors to be better informed of compliance issues and to identify further or remedial training requirements. The Data Quality reports will provide evidence for capability processes to be considered in the cases of repeated failures or non-compliance.

**LEGISLATION & REGULATION:**

- Force Information Security Procedure
- [Data Protection Act 2018](#)
- [Computer misuse Act 1990](#)
- [Freedom of Information Act 2000](#)
- [Human Rights Act 1998](#)