West Yorkshire
Fire & Rescue Service

Data Quality Policy

OFFICIAL
Ownership: Corporate Services
Date Issued: 15/05/2024
Version: 5.10   Status: Approved

Making West Yorkshire Safer
www.westyorksfire.gov.uk

Revision and Signoff Sheet

Change Record

Date	Author	Version	Comments
01/11/2007		1.0	First issued
01/08/2012	Pam Imeson	2.0	No changes – new template
01/06/2018	Alison Davey	3.0	Amendment of job titles
04/02/2022	Deb Wilson	4.0	Full review and update
08/03/2022	Deb Wilson	4.1	Accessibility updated
20/02/2023	Shashi Sumputh	5.0	Amendments to job titles and links
15/05/2024	B Croft-Nicholson	5.1	Amendments to job titles and HRH

Reviewers

Name	Version	Position	Organisation	Date
	4.0	Information Governance and Security Group	WYFRS	22/02/2022
Shashi Sumputh	5.0	Information Governance Manager	WYFRS	20/02/2023

Distribution

Name	Position	Organisation
All personnel		WYFRS

Document Properties

Item	Details
Document Title	Data Quality Policy
Author	Administrator
Creation Date	01/11/2007
Last Updated	20/02/2023

Contents

1 Definitions

Word/phrase/term/acronym	Meaning
Controls	Specific activities undertaken to reduce exposure to risk e.g., a data standards checklist.
C I M G	Corporate Information Management Group.
C S	Corporate Services.
D P O	Data Protection Officer.
Data	The reinterpretable representation of information in a formalised manner suitable for communication, interpretation, or processing. Source**: The Information and Data Quality ISO 8000-8**
Data quality	The degree to which data is appropriate and useful for a particular purpose. Source**: The Information and Data Quality ISO 8000-8**
Dataset	A collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer.
Data quality standards	Accurate, Complete, Relevant, Reliable, Timely, Valid.
E I R	Environmental Information Regulations.
F O I	Freedom of Information.
G D P R	General Data Protection Regulation.
I G S G	Information Governance and Security Group.
Information	Knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, which have a particular meaning within a certain context. Source**: The Information and Data Quality ISO 8000-8**
Information asset	A body of information defined and managed as a single unit so it can be understood, shared, protected, and exploited efficiently.
Information Asset Owner (I A O)	The nominated owner of the information asset who is responsible for making sure it's handled and managed appropriately i.e.; it's meeting its requirements and that risks and opportunities are monitored. The owner need not be the creator, or even the primary user of the asset, but they must have a good understanding of what the business needs from the asset, and how the asset needs to be able to fulfil those requirements.
Information Asset Register (I A R)	A comprehensive list of the information assets of an organisation.
L M	Line Manager.
S A R	Subject Access Request.
S I R O	Senior Information Risk Owner.
Validation	Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.

2 Summary of key points

Policy purpose: to provide an overarching, corporate approach to the management of our data quality. It provides a framework for us to ensure a high level of data quality within WYFRS.

Note: As our organisation generates a wide range of data for a variety of uses, this policy cannot provide detailed procedures or guidance for specific data processes. It will therefore make reference to generic stages of 'the data process' (see below) which are comparable with most business-specific processes. In addition, the policy will signpost where specific procedures or guidelines need to exist.

1. **INPUT:**
    - **Collect** data using various methods.
    - **Capture** manually or electronically.
    - **Check** data.

2. **PROCESS:**
    - **Transform** raw data into information.
    - **Transmit** to other systems if required.
    - **Validate** information.

3. **BUSINESS OUTPUT**
    - **Present or issue** to user.
    - **Update or amend** in line with reviews or feedback.

4. **STORAGE**
    - **Store** and retrieve data.
    - **Monitor** to required controls and standards such as retention and deletion.

Policy scope: Data quality is everyone's responsibility. This policy applies to all WYFRS data, whatever its purpose, form, or location. All data is important – although the level of importance will vary between the different information assets within our organisation. It also applies to third party and partner agency data supplied to us.

Definition and importance: The Information and Data Quality ISO 8000-8 defines data quality as 'The degree to which data is appropriate and useful for a particular purpose'. Unreliable data produces unreliable analysis, making informed decisions impossible — thereby undermining the public's confidence in us and threatening the reputation and growth of WYFRS.

Our Data Quality Standards: These are used across many organisations:

1. **Accurate**. (Correct).
2. **Relevant**. (Appropriate).
3. **Complete**. (Not missing).
4. **Reliable**. (Consistent).
5. **Timely**. (Prompt).
6. **Valid**. (Fit for purpose).

Our Data Quality Framework: If we are to achieve consistently high standards of data quality, leadership is essential, underscored by a comprehensive management framework, which includes:

- **Training and guidance**: To foster an organisational culture that values data quality, all staff should receive the appropriate communication, guidance, or training in relation to the data quality aspects of their work.
- **Established systems and processes**: These must be in place to ensure data is available in the required format - within timescales that sufficiently allow best use of the information as well as any action required.
- **Effective procedures and timescales:** All our data processes should be covered by clear procedures detailing what is required at each relevant stage and the steps involved.
- **Defined responsibilities**: The SIRO, DPO, IGSG, CIMG, CS, IAOs and LMs all have levels of responsibility. All staff are responsible for maintaining data quality standards, raising identified data quality issues with the appropriate business area, and addressing gaps in their ability to do this.
- **Monitoring**: The Information Asset Owner is responsible for ensuring that data quality is monitored, against the data quality standards, on a risk assessed basis. There are various monitoring activities that do this including controls, checks, validation, reporting and auditing.
- **Assurance**: Assurance controls are provided through scheduled external and internal audits.

Related Documents:

- Information Asset Risk Policy.
- The Role of the Information Asset Owner.
- Retention of documents.

3 Policy Purpose

Data quality is a fundamental component of the West Yorkshire Fire and Rescue Service Information Governance Framework. Our customers (external and internal) need to be able to trust the relevance, reliability, and validity of information sources, and have confidence that our data is complete, accurate and up to date. In order for us to demonstrate that we are meeting these needs, we must be able to identify and measure the quality level of our data by these standards.

This policy provides an overarching, corporate approach to the management of our data quality. It sets out our approach to ensuring that:

- There is a high level of data quality within West Yorkshire Fire and Rescue Service and a framework in place to maintain this.
- The importance, principles and standards of data quality are fully embedded across our organisation and are key considerations of all staff.
- We meet external and internal audit standards and requirements.

Note: As our organisation generates a wide range of data for a variety of uses, this policy cannot provide detailed procedures or guidance for specific data processes. It will therefore refer to generic stages of ‘the data process’ (see below) which are comparable with most business-specific processes. In addition, the policy will signpost where specific procedures or guidelines need to exist.

- **INPUT:**
    - Collect data using various methods.
    - Capture manually or electronically.
    - Check data.
- **PROCESS:**
    - Transform raw data into information.
    - Transmit to other systems if required.
    - Validate information.
- **BUSINESS OUTPUT:**
    - Present/issue to user.
    - Update/amend in line with reviews/feedback.
- **STORAGE**:
    - Store and retrieve data.
    - Monitor to required audit controls and standards such as retention and deletion.

This policy outlines the steps necessary to maintain high quality standards throughout the data processes that result in the production of our many business outputs such as:

- Information databases.
- Performance information.
- Risk/ operational/ financial plans and reports.
- Responses to public information requests e.g., FOI/ SAR/ EIR.
- Staff records e.g., personal details, contacts, payroll, Training and Competence records.
- Corporate web content (internal and external).
- Project.
- Policies and procedures.
- Training and guidance documents.
- Communications such as emails, briefings, publications, notices, meeting minutes etc.

Note: This list is not exhaustive.

4 Policy Scope

Data quality is everyone's responsibility. This policy applies to all West Yorkshire Fire and Rescue Service employees. Individuals who do not handle data or information as part of their role, still have a responsibility to ensure that any West Yorkshire Fire and Rescue Service data they may see or read complies with this policy’s standards.

It applies to all West Yorkshire Fire and Rescue Service data, whatever its purpose, form, or location. All data is important – although the level of importance will vary between the different information assets within our organisation.

The Information Asset Register is the database of all the information assets within West Yorkshire Fire and Rescue Service. It is a comprehensive list of the assets and related business requirements. In preparation for GDPR in May 2018, a full review was undertaken, and the register was updated to reflect all datasets (and their purposes) across West Yorkshire Fire and Rescue Service. It also received a substantial assurance opinion in April 2018 and January 2021. Data quality of the information assets is reviewed as part of the Information Governance Audits that are regularly carried out. This allows us, as an organisation to document our adherence with data quality requirements.

Note: As well as West Yorkshire Fire and Rescue Service data processes, this policy also applies to third party and partner agency data that is supplied to us.

5 Introduction to Data Quality

5.1 What data quality is and why it is important to us?

The Information and Data Quality ISO 8000-8 defines data quality as

The degree to which data is appropriate and useful for a particular purpose.

Poor data quality leads to:

- the inability to make informed decisions and the potential loss to reputation.
- poor judgements made in relation to our operational performance.
- non-compliance of regulations such as GDPR and a potential financial loss.
- poor customer service externally and the potential of bad publicity.
- poor customer service internally and the potential of low morale.
- lack of collaboration with our partner organisations and third-party contractors.

To achieve our ambition of ‘Making West Yorkshire Safer’ and our strategic priorities, we need to continuously adapt and improve what we do, without compromising public safety. To do this, we need good quality data to work smarter throughout the service.

Our customers, Authority members, and other external bodies use information to assess our performance. They need to have confidence in our decision making. In turn, we must have confidence in the consistency and quality of the data we use as the basis for making critical decisions.

In summary, unreliable data produces unreliable analysis, making informed decisions impossible — thereby undermining the public's confidence in us and threatening the reputation and growth of West Yorkshire Fire and Rescue Service.

6 What makes good data quality?

There are six key characteristics that are used across many public and private sector organisations to assess the quality of data. We refer to these as our data quality standards. Achieving these standards will satisfy us and our stakeholders that our data is of good quality and can be used with confidence.

1. **Accurate. (Correct)**
    - sufficiently accurate for its intended purposes.
    - captured once only, although it may have multiple uses.
    - based on facts not personal assumptions or opinions.
    - the aim should be 100% accuracy 100% of the time.

2. **Complete. (Not missing)**
    - Captured in full i.e., sufficient for its intended purpose, but not excessive.

3. **Relevant. (Appropriate)**
   - succinctly relevant to the purposes for which it is used.
   - meets current and potential users' needs.

4. **Reliable. (Consistent)**
   - reflects (as near as possible) its exact or true values i.e., reality.
   - stable and consistent data collection processes and definitions.
   - changes to data reflect reality and not variations in data collection approaches or methods.

5. **Timely. (Prompt)**
   - captured as quickly as possible after the event.
   - input on an ongoing basis, rather than being stored up for bulk input at the end of a period.
   - available for the intended purpose within a reasonable time.
   - retained only for the time it is serving its intended purpose, after which the relevant action (destroy, archive etc.) is taken.

6. **Valid. (Fit for purpose)**
   - in accordance with these standards and any other requirements, such as the correct application of any system rules or national / local definitions.
   - Where proxy data is used instead of actual data e.g., for training purposes, data satisfies the intended purpose.

7 Legislative Requirements

7.1 General Data Protection Regulation (GDPR)

Article 5 of the GDPR, states the six data protection principles that set out the main responsibilities for organisations. Five of these six principles relate to data quality, stating data should be:

1. Processed **lawfully, fairly and in a transparent manner** in relation to individuals.
2. Collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes.
3. **Adequate, relevant, and limited** to what is necessary in relation to the purposes for which they are processed.
4. **Accurate** and, where necessary, **kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.
5. Kept in a form which permits identification of data subjects **for no longer than is necessary** for the purposes for which the personal data are processed.

The sixth confirms that the controller shall be responsible for, and be able to demonstrate, compliance with the principles. The data controller within West Yorkshire Fire and Rescue Service is the Director of Corporate Services, and we all therefore have a legal duty as employees to demonstrate that we comply with the GDPR principles on their behalf.

7.2 Subject Access Rights

Also, under GDPR, individuals have Subject Access Rights i.e., the right to be informed whether West Yorkshire Fire and Rescue Service holds any personal data about them and a right to be provided with a copy of it within a month. It is therefore imperative that what we have recorded about them is in line with the data quality standards.

7.3 The Freedom of Information Act 2000

This legislation entitles members of the public to request information about West Yorkshire Fire and Rescue Service that is not already published on our website.

It is worth bearing these legislations in mind when capturing data or information, asking ourselves ‘if an individual requested any data or information, I had captured about them or our organisation, would I be satisfied that it was accurate, complete, relevant, reliable, timely and valid?

8 Our Data Quality Framework

If we are to achieve consistently high standards of data quality, leadership from the top of the organisation is essential, underscored by a comprehensive management framework, which includes:

1. Training and guidance
2. Established systems and processes.
3. Effective procedures and timescales
4. Defined responsibilities.
5. Monitoring
6. Assurance

8.1 Training and guidance

Data is created and then utilised for various reasons. However:

- The individual or system creating the data may not know how it will be utilised.
- The individual or system utilising the data may not know the context in which the data was created e.g., its origin, quality level, legality or meaning.

To foster an organisational culture that values data quality, all staff should receive the appropriate communication, guidance, or training in relation to the data quality aspects of their work, in particular:

- how this policy applies to them.
- the importance of good data quality and their own contribution to achieving it.
- the impact and consequences of poor data quality.
- how to carry out their data quality responsibilities for the systems/processes they are involved in.
- legal and statutory requirements and recognised good practice.
- if data must be in accordance with any locally or nationally set definitions.
- what business outputs are produced from captured data.

- any performance indicators /policies/decisions affected by the data they contribute.

8.2 Established systems and processes

Systems and processes must be in place to ensure data is available in the required format - within timescales that sufficiently allow best use of the information as well as any action required.

Where information will be extracted regularly, they must allow for efficient extraction and swift communication.

Each system or process will have an Information Asset Owner who is ultimately responsible for data quality. Where necessary, feedback should be provided for system/process improvements and/or staff development.

Staff, partners and third parties should be consulted when developing or implementing new information systems.

Data migration projects (direct or via partners/third parties) should always include a data cleansing review to ensure that:

- outdated and poor-quality data is not migrated to the new system.
- migrated data meets the required data quality standards.

8.3 Effective procedures and timescales

All our data processes should be covered by clear procedures detailing what is required at each relevant stage and the steps involved. They should:

- be easily available to all relevant staff.
- set out timescales so that all key dates can be observed.
- include steps required for identifying and correcting data errors.
- regularly reviewed and updated - normally annually.
- be designed so that they can be easily carried out by replacement staff.

8.4 Defined responsibilities

8.4.1 SIRO / Deputy Chief Fire Officer.

Overall strategic responsibility for data quality.

8.4.2 DPO / Director of Corporate Services.

Providing direction, support and advice to the Authority, Principal Officers, Heads of Service, and all departments in relation to their data protection (including quality) obligations.

8.4.3 Information Governance and Security Group (IGSG).

The protection and preservation of West Yorkshire Fire and Rescue Service’s information assets and to provide support to Information Asset Owners in respect of finding solutions to unresolved data quality issues.

8.4.4 Corporate Information Management Group.

Working with the Principal Officers or Heads of Department to oversee the implementation of this Data Quality policy.

8.4.5 Corporate Services.

Overseeing the Information Asset Register (IAR).

8.4.6 Information Asset Owners (IAOs).

Ensuring that the operational management of the data quality of their asset is undertaken i.e.:

- procedures and training guides reflect data quality requirements.
- monitoring is carried out on a risk assessed periodic basis and reported where necessary.
- appropriate audit trails can be produced.
- actions recommended by reviews are implemented and system upgrades are made where appropriate to validate data quality.
- appropriate data quality clauses are in any relevant third party/partner contract or agreement.
- there is a named individual who can deputise in their absence by (at least) maintaining the day-to-day asset functionality.

8.4.7 Line Managers

Ensuring that, where appropriate all their staff:

- have read and understood this policy.
- are fully aware of their data quality obligations and responsibilities.
- are competent to carry out their duties in line with this policy.
- are made aware of data quality responsibilities via job descriptions, appraisals, and inductions.

8.4.8 All staff

- Maintaining data quality standards.
- Raising any identified data quality issues with the appropriate business area.
- Identifying and addressing gaps in their ability to do this.

Note: Staff are obligated:

- legally (via GDPR and other data relevant legislation).
- contractually (via contracts of employment).
- ethically (via professional codes of practice).

8.4.9 Internal and external auditors

Reviewing and reporting on adherence with this policy and making recommendations to address any identified non-adherence.

8.4.10 Third parties and partners

It is essential that we have confidence in the quality of data supplied by third parties and partners e.g., data about a contractor's performance. We will ensure our agreements and contracts with partners and third parties include a clause relating to adherence with this Data Quality Policy. Any doubts about their data quality should be addressed with the organisation. Responsibility for data verification lies with the department receiving the information.

Non-adherence to this policy will be reported to the Director of Corporate Services. This will be done on an exception basis. Non-adherence by partners and third parties will also be pursued and rectified.

8.5 Monitoring

Incorrect, incomplete, irrelevant, unreliable, missing, out of date or invalid records provide an indication of data quality and can also point to underlying problems in the data process.

This framework ensures that the appropriate data quality monitoring is considered for each information asset. The Information Asset Owner is responsible for ensuring that data quality is monitored, against the data quality standards, on a risk assessed basis. They should identify the potential causes of risks to data quality that apply to their information asset, such as:

- A high volume of data transactions.
- Technically complex data transactions / reporting.
- Significant manual handling or manipulation of data.
- Issues identified though audit review.
- Inexperienced staff involved in data processing.
- New systems introduced to capture and or disseminate data / information.
- Known gaps in the control environment.

Note: This list is not exhaustive.

Key Risk Indicators (KRIs) need to be implemented and monitored together with the effective controls to deal with them. The data quality risk assessment will be unique to each information asset. Information asset owners should assess:

- How critical the information asset is to the business (the IAR has this information).
- What assurance they have that data quality is at the accepted level in relation to that.

The outcome of the assessment should determine the level and type of monitoring (if any) that is required.

8.5.1 Controls and checks

During the data process, it is imperative that adequate controls and checks are undertaken against the required standards. Such processes may include sample checks, checklists and report test runs that:

- check for duplicate or missing data.
- ensure that definitions and coding standards are adopted.
- ensure data quality standards have been met.

In order to reduce errors, data requirements within systems and processes must be designed, wherever possible, along the principle of ‘getting it right first time’ i.e., interfacing between different information systems, matching and consolidating data from multiple databases, etc.

8.5.2 Validation

Nevertheless, in complex processes, even where there are strong controls and checks, errors can still occur. Therefore, a validation procedure should exist in these cases. The frequency of validation checks will need to be appropriate to the frequency of data reporting.

Validation can be accomplished using some or all of the following methods:

- **Automated system validation:** systems programmed to check in full or in part the acceptability of the data. Where applicable, national definitions and coding standards should be incorporated into the validation functionality.
- **Synchronising information systems:** system functionality allowing any modifications made to source data to be replicated in other related systems, ensuring there are no inconsistencies between them.
- **Comparisons:** Looking at trends in the data compared with historical/alternative data sets.
- **Data cross checking:** which can also be performed on data held by different departments/systems/people.
- **Original sources spot checks:** The analysis of a random selection of records against source material or even people e.g., staff or service users.
- **Templates:** allow users to enter data in a consistent and coherent manner. They ensure that users enter all of the required information and prompt them in a logical format.
- **Data cleansing exercises:** usually before migrating to a new system or process.

It is extremely important that information being passed up the line for management action or submitted for audit is subject to at least one of the validation methods above.

8.5.3 Third parties and partners

Particular attention needs to be paid to data provided by external sources. When entering into contracts or agreements with third parties and partners who will provide us with information, Information Asset Owner’s must:

- communicate how their data quality responsibilities will be checked i.e.:
    - the format, presentation and collection frequency of their data must comply with our requirements.
    - they must share the same understanding of any specific data definitions.
    - all key dates for the submission of data must be adhered to.
- ensure that the data supplied is checked in the same way as internal data and that a clear audit trail to evidence validation checks is kept on file.
- include, wherever possible, a specific objective relating to data quality into all contracts or agreements.

8.5.4 Reporting

We will formally report on data quality as follows:

- regular reporting of issues arising from data quality reviews through Information Asset Owners. Where an issue relating to data quality cannot easily be resolved through guidance and coaching at the specific stage of the process, it will be reported by the Information Asset Owner to the Information Governance and Security Group and ultimately, if still not resolved, to the Director of Corporate Services.
- outcomes of internal audit reviews will be shared with the relevant risk owners and will be reported to the Audit Committee.

8.5.5 Policy implementation and review

The Head of Corporate Services has responsibility for the implementation of this policy, by ensuring that:

- all staff are made aware of it.
- all staff affected by section 8.4 are aware of their responsibilities in respect of it.
- the policy is reviewed and updated every three years - or earlier if it is impacted by any key changes in external or internal requirements.

8.5.6 Assurance

8.5.6.1 Internal audits

- **Kirklees Council**
  Kirklees Council provide internal assurance controls through scheduled audits - which may include data quality. Any audit recommendations are incorporated into the data quality framework and this policy.

- **Service Assurance**
  The service assurance framework within West Yorkshire Fire and Rescue Service uses departmental self-assessment audits to ensure that our processes and procedures are being undertaken to the required standards. Data quality is included as a standard within the framework and is an opportunity for departments to review their data quality responsibilities.

8.5.6.2 External audits

Periodic inspectorate audits are carried out by His Majesty's Inspectorate of Constabularies and Fire and Rescue Services (HMICFRS), which may include data quality. Any errors discovered during an audit will be corrected within established timescales and any improvement actions will be acted upon in order to continuously improve our approach to data quality.

Information Asset Owners should provide data quality advice and information to the auditors when requested.

9 Related Documents

- Information Asset Risk Policy.
- The Role of the Information Asset Owner.
- Retention of documents.

10 Appendix: The data quality risk assessment process

1. What data am I responsible for?

- Review the Information Asset Register and other department processes and systems to create a list and assess each one separately as follows:

2. How critical is it to West Yorkshire Fire and Rescue Service?

- Consider the purpose of it and the business need.
- Check its criticality rating on the Information Asset Register.
- Taking both into account, assign a high, medium, or low critical status and then re-prioritise the list.

3. What existing controls are already in place?

- What administrative, technical, and physical controls exist to maintain the data quality of the asset?

At this point it may be sufficient to rely on existing controls that have already been based on criticality e.g., full checks may already be in place because the output is considered critical to the organisation. If further review is needed, continue with this process.

4. Identify and list risks

- What could reasonably be expected to cause harm by this asset containing poor data quality?
- I.e., data that is inaccurate, incomplete, irrelevant, unreliable, missing, out of date or invalid?
- Have data quality incidents occurred previously?

5. Evaluate the risks and assign a risk rating

RISK ASSESSMENT

LIKELIHOOD	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		SEVERITY			

RISK RATING
HIGH
MEDIUM HIGH
MEDIUM LOW
LOW

Consider the severity and likelihood of harm after being exposed to a risk. Ask:

If WYFRS was exposed to this risk, how bad would the severest harm be? (Severity).

Note: In order to answer this effectively you have to presume that the risk and effect is inevitable.

1. Fatal.
2. Major - serious damage to reputation.
3. Minor - reversible damage which may require attention but limited ongoing treatment. This is less likely to involve significant effect.
4. Negligible - little or no lost time.

Likelihood: How likely is WYFRS to be harmed if exposed to the risk?

Note: This should not be confused with how likely the risk is to occur.

1. Very likely - exposed to risk continuously.
2. Likely - exposed to risk occasionally.
3. Unlikely - could happen but only rarely.
4. Highly unlikely - could happen, but probably never will.

6. Decide on the most effective protection control(s).

Use a hierarchy of controls to choose the right control measure applicable to the risk rating.

- High - control all serious risks immediately e.g., check every input.
- Medium High - frequent specific controls e.g., check 10 per week for specifics.
- Medium Low - sporadic controls e.g., random checks.
- Low – no direct control necessary e.g., existing periodic audits is sufficient control.