Data Quality Policy

March 2014
This Data Quality Policy should be read in conjunction with, but not exclusively with, the following:

- Information Governance Framework;
- Information Governance Strategy and Policy;
- Records Management Policy;
- Data Protection Policy;
- Freedom of Information Policy;
- Personal File Guidance;
- ICT Security Policy;
- Communications Strategy;
- Consultation Strategy;
- Media Strategy;
- Social Media Policy;
- Discipline Policy & Procedure;
- Publication Scheme;
- Code of Conduct and Code of Accountability for NIFRS Board Members *(NB: to be formally adopted by Board)*; and
- Staff Code of Conduct.

Relevant documents above will be reviewed in line with the requirements of the Information Governance Framework, Strategy and Policy.
1 INTRODUCTION

Data quality is one of the key areas covered by NIFRS Information Governance Framework that sets out the agreed approach for managing information as an asset. Information Governance is concerned that the information used by NIFRS is:

- held securely and confidentially;
- obtained fairly and lawfully;
- recorded accurately and reliably;
- used effectively and ethically; and
- shared appropriately and legally.

1.1 Everyone’s Concern

Ensuring that data and information is of an appropriate quality for its purpose underpins the usefulness of information. Poor data quality can have a negative impact on all NIFRS functions from service provision through to performance management and decision-making, as well as affecting overall efficiency. Everyone who collects or processes data has an important role to play in maintaining data quality.

1.2 Legal Compliance

The requirement to maintain quality of personal information is also covered by legislation, for example, Data Protection Act 1998 Principle 3 specifies that personal data shall be adequate, relevant and not excessive. Principle 4 specifies that personal information should be accurate and, where necessary, up-to-date.

1.3 Transparency

Data quality can be seen as the aspect of information management that focuses on information’s fitness for purpose. With increasing use of joined up information systems, information sharing and openness to public scrutiny, data quality is an essential aspect of Information Governance.

This document describes the policy, procedures, guidance and standards relating to NIFRS data quality. The standards set out in this Policy provide general principles for the management of data quality which are applicable to all types of data.

2 SCOPE

This Policy applies to all data within NIFRS, including data captured by NIFRS; gathered from partners or external data sources; provided to the public, partners, Government or others, but is primarily aimed at:

- Data for public service provision where NIFRS is dependent on the regular collection and maintenance of quality service user data to provide an efficient and effective service.
• Information provided for internal management and external reporting purposes.

• Information that will be shared with or received from other agencies

• Information that is published in print or via the web.

It applies to all those involved in collecting and entering data and those responsible for the management of those information assets. It should be read in conjunction with the Information Governance Framework, Strategy and Policy and Records Management Policy.

3 POLICY

The Policy detail is set out in Appendix 1 - Data Quality Framework, showing the detailed requirements in terms of:

• Management Arrangements;
• Training and Awareness;
• Documented Standards and Procedures;
• New and Changed Systems; and
• Policy Implementation and Compliance.

4 DEFINITIONS

This Policy uses the terms data, information and records. Data is the raw input from which information of value is then derived. Records (manual or digital, unstructured) are sets of information kept to evidence performance of a function. Records in the ICT usage sense are elements of a structured database system. Whichever term is used the need for quality collection, entry and maintenance processes is the same.

5 DATA QUALITY CHARACTERISTICS

This Policy aims to ensure the achievement of quality data by requiring the following:

<table>
<thead>
<tr>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data should be sufficiently accurate for its intended purposes.</td>
</tr>
<tr>
<td>Data should be captured on the principle of ‘getting it right first time’, so captured once, captured as close to the point of activity as possible, with clear and simple actions and only limited, if any, manual intervention (eg, administration, data cleansing).</td>
</tr>
<tr>
<td>Accuracy is likely to be higher if staff who provide data are aware of its importance and quickly have access to information based upon it, especially if they obtain some benefit for their effort in securing the quality of that data, for example, by receiving relevant</td>
</tr>
</tbody>
</table>
performance information in return.

- Accuracy is a balance between the importance of data and the cost of collection. Where there are compromises on accuracy for the sake of cost, the limitations of data should be clear to the users. Compromise is unlikely to be appropriate in the case of data supporting published performance indicators.

<table>
<thead>
<tr>
<th>Validity</th>
<th>Data should be recorded and used consistently, in compliance with relevant requirements, rules or definitions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability</td>
<td>Data should reflect stable and consistent data collection processes, or where changes or differences are necessary, sufficiently documented and understood so information produced is stable and consistent.</td>
</tr>
<tr>
<td>Timeliness</td>
<td>Data should be captured as quickly as possible after the event, and must be available for its intended use within a reasonable time period.</td>
</tr>
<tr>
<td>Relevance</td>
<td>The purpose for capturing data must be understood and the data captured should be relevant to that purpose. This entails periodic review of data capture requirements.</td>
</tr>
<tr>
<td>Completeness</td>
<td>Identification and highlighting missing, incomplete or invalid records can provide an indication of data quality and highlight ways in which the data capture process can be improved.</td>
</tr>
</tbody>
</table>

6 **OBJECTIVES OF THE POLICY**

The purpose of this Policy is to set out NIFRS’ requirements for ensuring that the data collected is of an appropriate quality for the uses to which it is put, or might be put in the future. The objectives of the Policy are:

- To instil confidence that all data and information that is used from operational information to strategic decision-making information, including that which is shared with other organisations or made public.

- Enhanced efficiency and effectiveness arising from the reduction of errors and improved accuracy and reliability resulting from a more structured approach to improving data quality.

- To underpin the better use of information to support services and improve accessibility and transparency for the wider community and partners.

7 **RISK MANAGEMENT**

The approach is, as for Information Governance generally, squarely centered on risk assessment.
Examples of some of the risks associated with data quality problems are:

- Negative consequences, financial and other, as a result of submitting inaccurate or misleading data in statutory or regulatory returns.
- Misleading external and internal impressions of organisational performance.
- Inappropriate decision-making and inefficient service provision.
- Reputational damage.
- Harm to an individual or group of individuals where NIFRS has a duty to protect.
- Undermining NIFRS’s relationship with its partner agencies.
- Regulatory action and fines from the Information Commissioner for breaches of DPA or FOI legislation.

Risk management aspects within the Data Quality Framework will follow the same broad principles and processes as set out for Corporate Risk Management Strategy/Policy/Procedure and related Assurance Framework.

8 DATA QUALITY AND RECORDS MANAGEMENT

There is a close relationship between data quality and records management, the former being focused on data collection and the latter on collections of records. Sometimes these overlap where data input or recording is less structured.

For example, this Policy focuses primarily on data collection in structured ICT based systems, but it will be apparent that widespread use is made of ‘Free Text’ or ‘Comments’ fields, which do not lend themselves to data validation.

Staff recording in these fields will need additional guidance on what is appropriate to record as it is sometimes overlooked that any information recorded may be required to be disclosed under FOI or DPA legislation. Guidance on how to record may be given in local recording practice procedures.

The Data Quality Policy and Records Management Policy should be read together because they are complementary and form a full management approach to the ‘information life cycle’ for NIFRS.

9 ROLES AND RESPONSIBILITIES

9.1 NIFRS Board

Overall responsibility for the efficient administration of the Information Governance, including Data Quality and Records Management, lies with the Board.
9.2 **Audit, Risk and Governance Committee**

This Board Committee receives progress reports on Data Quality issues and will report to the Board accordingly.

9.3 **Accounting Officer**

The Accounting Officer has overall responsibility for Information Governance within NIFRS. He/She is responsible for the management of Information Governance, including Data Quality and Records Management, and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Information Governance provides a framework to ensure information is used appropriately and is held securely.

9.4 **SIRO**

The Senior Information Risk Owner (SIRO) has overall corporate responsibility for the Information Governance Framework, including Data Quality and Records Management.

9.5 **Personal Data Guardian**

The Personal Data Guardian is the responsible officer for the purpose and manner in which personal data is collected, processed, stored, shared and dispensed with.

9.6 **Directors and Heads of Department**

Day-to-day responsibility for administration and compliance with this Policy is delegated from the Board through the Accounting Officer to respective Directors/Heads of Departments for their service area.

9.7 **Information Management & Governance Group**

The Information Management & Governance Group, made up of individuals that are suitably senior and/or with necessary expertise, will be delegated with the responsibility for the implementation and monitoring of Information Governance across NIFRS.

9.8 **Information Asset Owners (IAOs)**

The Information Asset Owners (IAOs) are responsible to their Head of Department or Director for liaison with the Information Management & Governance Group on all matters concerning administration of this Policy and are:

- To work with the Director or Head of Department to ensure compliance in respect to systems within the Directorate.
- To work with the Director or Head of Department to ensure awareness of the need for Information Governance within the organisation, and to ensure that the control and handling of information within the Department or Station does not contravene any appropriate legislation or NIFRS procedures.

- To ensure that Data Quality requirements are included in all information systems.

9.9 **Managers**

Managers are responsible for ensuring that staff under their direction and control, are aware of the policies, procedures and guidance laid down by the Senior Information Risk Owner (SIRO) through the Information Management & Governance Group, and for checking that those staff understand and appropriately apply policies, procedures and guidance in respect of Information Governance in carrying out their day-to-day work.

9.10 **All Staff**

It is the responsibility of all staff to process information in accordance with the Data Protection Act 1998 and to adhere to the policies, procedures and guidance that are laid down by NIFRS for Information Governance and Security.

10 **COMPLIANCE AND BREACHES**

The requirements for compliance monitoring are set out in the Data Quality Framework.

Any breaches of the principles of this Policy should be reported to the Senior Information Risk Owner (SIRO) via SIRO@nifrs.org. Data errors should be reported through normal channels. Failure to comply with this Policy may result in disciplinary action under the auspices of the Discipline Policy & Procedure.

11 **POLICY REVIEW**

This Policy will be reviewed annually, or as and when changes occur legislatively or within NIFRS.
### Appendix 1

#### DATA QUALITY FRAMEWORK

<table>
<thead>
<tr>
<th>Management Arrangements</th>
<th>Training and Awareness</th>
<th>Documented Standards and Procedures</th>
<th>New and Changed Systems</th>
<th>Policy Implementation and Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Audit, Risk &amp; Governance Committee will receive progress reports on the implementation of this Policy and data quality issues arising.</td>
<td>There will be effective communication and awareness of this Policy, the implications of poor data quality and the Policy's requirements.</td>
<td>Data quality will be embedded in business processes.</td>
<td>The identification and consideration of data quality risks and requirements will be undertaken as part of the risk management process for projects and programmes.</td>
<td>Data collection and validation activities will be regularly monitored and data quality reports routinely considered by senior management.</td>
</tr>
<tr>
<td>The Data Quality Policy and the Records Management Policy together form a comprehensive management approach through the Information life cycle.</td>
<td>Appropriate skills training for all staff with assigned responsibility for information quality and records management.</td>
<td>There will be documented requirements, definitions and rules. This will include appropriate national data standards and the data requirements of partner agencies with whom NIFRS shares information.</td>
<td>Data migration must include data cleansing where necessary. System acceptance testing will include data validation and data quality testing.</td>
<td>Assessment of ongoing compliance with this Data Quality Framework will be overseen by the Information Asset Owner.</td>
</tr>
<tr>
<td>The Senior Information Risk Owner (SIRO) will have overall corporate responsibility for Data Quality and Records Management.</td>
<td>Periodic refresher training and inclusion in employee performance reviews where appropriate.</td>
<td>Data quality risks and countermeasures will be reviewed annually or as required by circumstances.</td>
<td>There will be evidence of all data quality issues being resolved prior to live implementation.</td>
<td>Quarterly compliance information will be provided as part of the Information Asset Register record return and will be reported to the SIRO and Audit, Risk &amp; Governance Committee.</td>
</tr>
<tr>
<td>Management Arrangements</td>
<td>Training and Awareness</td>
<td>Documented Standards and Procedures</td>
<td>New and Changed Systems</td>
<td>Policy Implementation Monitoring and Compliance</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------</td>
<td>-------------------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>The Information Asset Owners (IAOs) will ensure that all Information Quality and Record Management roles are identified, assigned and co-ordinated by lead managers, for the Information Assets that they control.</td>
<td>All staff entering data will be trained to collect and record service user information, check the information with an appropriate source and report errors or omissions.</td>
<td>Large-scale data collection exercises and external returns will always be supported by data quality procedures.</td>
<td>Data quality reporting will be built into processes wherever possible.</td>
<td>Data quality controls and measures are subject to regular review.</td>
</tr>
<tr>
<td>Responsibility will be assigned and documented to managers and staff for ensuring the accuracy of service user information for all systems that support service provision.</td>
<td>All staff will be alert to potential data quality problems and report them to their line manager.</td>
<td>Data quality procedures will be available to all staff involved in data collection.</td>
<td>Data quality should be considered as part of all information sharing/data exchange arrangements (internal or external) to ensure that exchanged data is of appropriate quality. For internal sharing, it is important that additional copies or versions of data are not created unnecessarily.</td>
<td></td>
</tr>
<tr>
<td>The task of reconciling service user records in any different and unsynchronised databases in use to support services will be assigned to relevant staff.</td>
<td>Line managers will support staff in complying with this Policy and any local procedures in place.</td>
<td>Any data quality issues arising from the wider potential usage of data/information, including availability under ‘open data’ arrangements, will be considered and addressed at the project stage.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>