Information Governance
Strategy & Policy

March 2014
This Information Governance Strategy & Policy should be read in conjunction with, but not exclusively with, the following:

- Information Governance Framework;
- 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 & Policy.
1 INTRODUCTION

Information Governance is a framework to bring together all of the requirements, standards and best practice that apply to the handling of information. It allows organisations and individuals to ensure that information is accurate, dealt with legally, securely, efficiently and in order to deliver the best possible service.

This Information Governance Strategy & Policy supports the principles of the Information Governance Framework which is based upon national best practice models including the Health & Social Care (HSC) Information Management Controls Assurance Standard.

Through the Information Management Controls Assurance Standard, NIFRS can ensure that it maintains information in a manner that effectively services its needs and those of its stakeholders in line with appropriate legislation.

2 STRATEGIC AIMS

Information is a vital asset, in terms of both the management of individual customers and the efficient management of services and resources. It plays a key part in corporate governance, service planning and performance management.

NIFRS recognises the importance of maintaining an appropriate and robust system of Information Governance Management so as to underpin and support NIFRS in the exercise of its functions and in order to maintain public confidence.

2.1 Aims

The aims of this document are to maximise the value of organisational assets by ensuring that data is:

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

To protect NIFRS’ information assets from all threats, whether internal or external, deliberate or accidental, NIFRS will ensure that:

- information will be protected against unauthorised access;
- confidentiality of information will be assured;
- integrity of information will be maintained;
- information will be supported by the highest quality data;
- regulatory and legislative requirements will be met;
- business continuity plans will be produced, maintained and tested;
- information security training will be available to all staff; and
- all breaches of information security, actual or suspected, will be reported to and investigated by the Senior Information Risk Owner (SIRO).
NIFRS aims to work collaboratively with partner agencies to ensure any Information Governance issues which span more than one organisation are handled effectively and appropriately.

3 POLICY

NIFRS recognises the need for an appropriate balance between openness and confidentiality in the management and use of information and fully supports the principles of corporate Information Governance and recognises its public accountability.

3.1 Principles

This document is founded upon the Values and Principles as contained within the Information Governance Framework. These in turn support the values and priorities of the organisation.

<table>
<thead>
<tr>
<th>VALUES</th>
<th>Compliance and Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparency</td>
<td>Adhering to the appropriate legislative requirements to minimise the risk</td>
</tr>
<tr>
<td>Transparency</td>
<td>to public information through inappropriate use, unauthorised access or</td>
</tr>
<tr>
<td>Transparency</td>
<td>misuse.</td>
</tr>
<tr>
<td>Openness</td>
<td>Making information more available to benefit the whole community.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Confining access to those with specific authority to view it.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Safeguarding the accuracy and completeness of information and ensuring</td>
</tr>
<tr>
<td>Integrity</td>
<td>the correct operation of all systems, assets and networks.</td>
</tr>
<tr>
<td>Accessibility</td>
<td>Ensuring that information is available and delivered to the right person,</td>
</tr>
<tr>
<td>Accessibility</td>
<td>at the right time.</td>
</tr>
<tr>
<td>Authenticity</td>
<td>Ensuring that information and records are credible and authoritative.</td>
</tr>
<tr>
<td>Reliability</td>
<td>Ensuring information and records can be trusted as a full and accurate</td>
</tr>
<tr>
<td>Reliability</td>
<td>representation of the transactions, activities or facts.</td>
</tr>
<tr>
<td>Accountability</td>
<td>Ensuring there is an appropriate management framework in place to effectively implement information governance policies, programmes, protocols and guidelines.</td>
</tr>
</tbody>
</table>

NIFRS aspires to reach the highest standards included within the Information Governance Framework and is committed to using the HSC Information Management Controls Assurance Standard, and self-assessing against it, to achieve this.

There are a number of key interlinked strands to the Information Governance Policy:

- Managing Information Governance;
- Information Security;
- Information Compliance (including Data Protection and Freedom of Information);
- Information Quality Assurance;
- Records Management; and
- Information Sharing.

4 RESPONSIBILITIES

4.1 NIFRS Board

Overall responsibility for the efficient administration of Information Governance lies with the Board.

4.2 Audit, Risk & Governance Committee

This Board Committee receives progress reports on the implementation of the Policy and Data Quality issues and will report to the Board accordingly. This Committee will appoint a suitable Information Governance Champion.

4.3 Accounting Officer

The Accounting Officer has overall responsibility for Information Governance within NIFRS. He/She is responsible for the management of Information Governance 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.

4.4 SIRO

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

4.5 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.

4.6 Directors and Heads of Department

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

4.7 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 the Organisation. The work undertaken
will be in line with the Group’s Terms of Reference as detailed at Appendix 1. The Group will report to the Senior Information Risk Owner (SIRO).

4.8 **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 the Framework/Strategy/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.

4.9 **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.

4.10 **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.

5 **INFORMATION GOVERNANCE REPORTING STRUCTURE**
The Information Management & Governance Group reports through the Corporate Management Team to the Audit, Risk & Governance Committee on all matters concerning Information Governance.

Associated Risks for Information Governance will follow the same broad principles and processes as set out for the Corporate Risk Management Strategy/Policy/Procedure and related Assurance Framework.

6 MANAGING INFORMATION GOVERNANCE

The development and implementation of an appropriate Information Governance infrastructure to be delivered across NIFRS is fundamental to the successful implementation of the Framework. It is necessary to provide ownership and advocacy at corporate, managerial and operational levels throughout the organisation.

6.1 Managing Information Governance Objectives

The Information Governance Strategy & Policy will be co-ordinated, publicised and monitored by the Information Management & Governance Group supported by the Terms of Reference (Appendix 1).

Corporate and managerial responsibilities for Information Governance across the organisation will be clearly defined.

An approved Information Governance Improvement Plan will be implemented, managed and monitored by the Information Management & Governance Group to ensure that all information is managed effectively and risks are reduced.

NIFRS policies and procedures will be regularly reviewed and kept up-to-date to reflect the ongoing development of national and international standards, new legislation, changing working practices and Government initiatives and best practice.

Staff training needs for Information Governance will be assessed, evaluated and action taken to ensure that they are delivered appropriately. The following chart shows the linkage between training and the other key strands within Information Governance.
7 INFORMATION SECURITY

Information Security is a key area in NIFRS’ overall Information Governance Framework that covers the wider needs of information management, including records management and data quality. NIFRS has adopted ISO 27001 and ISO 27002 Standards into its ICT Security Policy. Compliance with ISO 27001 will ensure compliance with Information Governance requirements.

7.1 Information Security Objectives

Adherence to the policies and procedures put in place, following the principles of the international standard, to protect information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction, will deliver information security compliance.

Information security is the responsibility of all managers and staff. NIFRS maintains an ICT Security Policy that sets out in more detail everyone’s responsibilities, approved guidelines and best practice.

NIFRS has established and maintains policies and procedures for the effective and secure management of its information assets and resources.

The organisation promotes effective confidentiality and security practice to its staff through policies, procedures, induction and training.

NIFRS has established and maintains formal incident reporting procedures and monitors and investigates all reported instances of actual or potential breaches of confidentiality and security.

NIFRS will seek to undertake or commission regular assessments and audits of its information and IT security arrangements.
8  INFORMATION COMPLIANCE

There is a legal framework which governs information products and NIFRS must be compliant with it. The organisation handles and processes large volumes of confidential and sensitive information about individuals and must deal with this lawfully and ethically. Failure to comply could endanger individuals and can also increase risk, the chances of litigation and the loss of reputation.

8.1  Information Compliance Objectives

NIFRS has an Information Governance Framework. Through our commitment to sharing information, NIFRS intends not only to fulfil any legal obligations but also to promote a spirit of openness and accessibility.

Individuals have the right to request access to information about them. Disclosure of such information will be in line with the Data Protection Policy. NIFRS has a written procedure which covers such Subject Access Requests and the relevant staff will be appropriately trained. The effectiveness of the procedure will be monitored and evaluated.

NIFRS has established and maintains policies and procedures to ensure compliance with Data Protection, Freedom of Information and Environmental Information Regulations.

8.2  Information and Human Rights Legislation

NIFRS has established and maintains policies and procedures for the controlled and appropriate sharing of customer information with other agencies, taking account of relevant legislation.

NIFRS ensures effective confidentiality and security practice to its staff through induction and training. The organisation undertakes or commissions annual assessments and audits of its compliance with legal requirements.

8.3  Information Quality Assurance

Information quality is an important part of the Information Governance Framework in terms of data quality and integrity. Quality is generally defined as ‘fit for purpose’ and all staff need to ensure that data is relevant and accurate. Good data quality means that data is recorded in full, as accurately as possible and in a timely manner. Timely data entry will help avoid discrepancies and inaccuracies. Where it is not possible to record data in real time, this data should be recorded as soon after the event as possible.

8.4  Information Quality Assurance Objectives

NIFRS has established and maintains policies and procedures for information quality assurance and the effective management of records. It aims to undertake or commission annual assessments and audits of its information quality and records management arrangements.
Managers have responsibility to take ownership of, and seek to improve, the quality of information within their services.

Wherever possible, information quality is assured at the point of collection.

Data standards have been set through clear and consistent definition of data items, in accordance with national standards.

The organisation promotes information quality and effective records management through policies, procedures/user manuals and training.

9 RECORDS MANAGEMENT

Records Management covers the process of creating, describing, using, storing, archiving and disposing of organisational records according to a defined set of Standards (usually ISO 15489). Compliance with this fundamental component of the Information Governance Framework will ensure that NIFRS adheres to statutory information access requirements.

9.1 Records Management Objectives

NIFRS will establish and maintain policies and procedures for records management.

Records standards will be set through the identification of best practice and in accordance with national standards and initiatives.

NIFRS aims to undertake or commission annual assessments and audits of its record management systems.

NIFRS will maintain a Records Retention Schedule together with policies for the management of manual and electronic corporate records.

10 INFORMATION SHARING

Information Sharing covers the proper governance of information sharing practice across the organisation. It is an essential component given that it deals with business activities involving the potential for sharing personal information about our customers, staff and other stakeholders. Ensuring that our practice is of the highest standard, meeting with regulatory mechanisms, such as the Data Protection and Human Rights Acts together with the Common Law Duty of Confidentiality, is essential in order to instil confidence amongst those whose personal information is involved in such business processes.

10.1 Information Sharing Objectives

An agreed Data Sharing Protocol Guidance will be put in place which will determine the principles we seek to achieve, the operational procedures that need to be followed and the considerations that must be given for legislative compliance.
A standardised, documented approach to information sharing will be implemented with appropriate guidance and templates to support it.

All information sharing agreements will be completed in full, setting out the justification for each sharing exercise, particularly the legal case for such agreements.

All information sharing agreements will be added to the Strategic Partnership Register maintained by the Planning & Corporate Affairs Directorate. The Register will be monitored to ensure that the partnerships and agreements are current and remain effective.

NIFRS maintains policies and procedures to ensure compliance with the Data Protection and Human Rights Legislation. Breaches of the Legislation will be reported to the Information Commissioner and internally to the Audit, Risk & Governance Committee.

NIFRS undertakes or commissions annual assessments and audits of its policies and arrangements for openness and confidentiality.

NIFRS promotes codes of openness and confidentiality to its staff through policies, procedures and training.

11 ASSESSMENTS, WORK PLANS AND IMPLEMENTATION ARRANGEMENTS

11.1 Assessment

The Information Management & Governance Group is responsible for ensuring an assessment of compliance, as detailed in the Information Governance Toolkit, is undertaken each year. Annual work/development plans are produced and these are considered by the Information Management & Governance Group at intervals throughout the year.

The Information Governance Toolkit requirements are grouped under the following criteria:

- Information Governance Management Framework;
- Information Risk Policy and Information Risk Management Strategy;
- Records Management;
- Freedom of Information Act 2000;
- Personal Information;
- Information Governance awareness and training;
- Confidentiality and Data Protection requirements;
- Information quality;
- Contractual arrangements;
- Information Life Cycle Management; and
- Individual requests for access to personal data.

11.2 Adherence

It is the responsibility of the Information Management & Governance Group to ensure that NIFRS adheres to its Information Governance
Strategy & Policy. For Information Security matters, NIFRS will seek advice and support from the Information Management & Governance Group with input from the IT Department.

11.3 Compliance and Breaches

Any breaches of the principles of this Strategy & 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.

11.4 Terms of Reference

The Terms of Reference of the Information Management & Governance Group are attached at Appendix 1.

11.5 Accountability

The Information Management & Governance Group reports to and is accountable to the Senior Information Risk Owner (SIRO).

11.6 Review

This Policy will initially be reviewed annually until substantive compliance is achieved; thereafter it will be reviewed every 3 years.
APPENDIX 1

INFORMATION MANAGEMENT & GOVERNANCE GROUP
TERMS OF REFERENCE

1 Purpose

The purpose of this Group is to provide advice and assurance to the Director of Planning, Performance & Governance on all matters concerning Information Governance.

2 Definition

Information Governance is a framework to bring together all of the requirements, standards and best practice that apply to the handling of information. It allows organisations and individuals to ensure that information is accurate, dealt with legally, securely, efficiently and in order to deliver the best possible service. The principles of Information Governance which is an organisational wide initiative provides a consistent way for employees to deal with many different information handling requirements.

3 Outcome

NIFRS must achieve HSC Controls Assurance Compliance at the levels mandated and be able to evidence same.

4 Objectives

4.1 To ensure that NIFRS has effective policies and management arrangements covering all aspects of Information Governance in line with the organisation’s overarching Information Governance Policy, ie:

- Management of Information Governance;
- Information Security (including confidentiality, integrity and availability);
- Information Compliance (eg, Data Protection Act);
- Information Quality Assurance;
- Records Management; and
- Information Sharing.

4.2 To ensure compliance with Information Governance requirements placed on the organisation, particularly by the Information Governance Framework, to develop action plans where compliance is less than 100% and monitor their implementation.

4.3 To ensure that NIFRS undertakes or commissions annual assessments and audits of its Information Governance policies and arrangements.

4.4 To establish annual Information Governance Framework Improvement Plans, secure the necessary implementation resources and monitor the implementation of those plans.
4.5 To receive and consider reports into breaches of confidentiality and security and where appropriate undertake or recommend remedial action.

4.6 To ensure all relevant risks are recorded on the Corporate Risk Register.

4.7 To report to the Audit, Risk & Governance Committee, CMT and other working groups in order to promote Information Governance issues.

4.8 To ensure full and effective liaison with all external organisations such as the Information Commissioner, local authorities and other relevant organisations.

4.9 To formulate and receive guidance from such supporting committees or groups as appropriate.

4.10 To report to the Corporate Management Team on Information Governance issues and to carry out such other tasks as may be required of it by the Director of Planning, Performance & Governance.

4.11 To identify where new policies and procedures are required or are in process of implementation and to assign responsibility for overseeing implementation of each policy and procedure.

5 Accountability

The Group reports to the Director of Planning, Performance & Governance who is the Senior Responsible Officer for Information Governance.

6 Membership

The Group membership will consist of nominated uniform and support personnel, staff with appropriate specialist roles and a Project Manager.

7 Meetings and Reporting

The Group will meet as often as necessary. Minutes of each meeting will be circulated within one week of the meeting.

8 Approval and Review

In line with these Terms of Reference, an Information Management & Governance Working Group has been established to deliver initial information project requirements.

The management of this going forward is yet to be determined.