**NHS Education for Scotland**

**Policy Document**

# Information Governance Policy

YOU CAN READ OR DOWNLOAD THIS DOCUMENT FROM THE NES INTRANET. WE CAN ALSO PROVIDE THIS INFORMATION BY EMAIL, IN

LARGE PRINT, ON AUDIO TAPE OR CD, IN BRAILLE AND IN OTHER

LANGUAGES

## 1. Introduction

NHS Education for Scotland (NES) recognises the importance of our information assets, both in terms of delivering workforce development and educational support to the NHS in Scotland, and in the efficient management of services and resources. Information governance plays a key part in supporting educational and research governance, service planning and performance management.

It also gives assurance to the organisations and individuals we work with that information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible service and to meet NES’s legal, policy and good practice responsibilities

NES will establish and maintain policies and procedures to ensure compliance with requirements contained in the NHS Scotland *Information Governance Standards*  and *Information Assurance Strategy.*

## 2. Purpose

The purpose of this document is to set the high-level framework within which the NES Board can monitor NES’ performance and compliance in information governance, and to provide an overview of responsibilities and sources of more detailed procedures for all NES staff.

## 3. Scope

The policy applies to all the business information received, created or held by NES, including, but not restricted to:

* Research and policy information;
* Operational and financial information;
* Personal information relating to health practitioners, trainees, trainers, contractors and employees;
* Organisational and corporate governance information.

The policy applies to all the formats of information held by NES, including, but not restricted to:

* Structured database records;
* Unstructured documents held on computer network drives, hard drives, mobile devices or removable media;
* E-mail held on current and ‘archive’ systems;
* Information published on the internet or intranet by NES;
* NES-originated or owned content on social media platforms;
* Paper records and working documents;
* Microfilm, microfiche and electronically-scanned documents;
* Information held outside NES premises or systems on our behalf; including on social media platforms and web-based systems;
* NES business information held offsite by NES employees engaged in home/flexible working;
* Information sent by e-mail, facsimile (fax) or other communications method;
* Images, audiovisual content, digital dictation and voice mail.

## 4. Policy linkages

The *Essential Criteria* from the relevant Standards informed the *Information Governance Standards* which have been used to structure the substantive content of this Policy (sections 5 to 14).

http://www.elib.scot.nhs.uk/SharedSpace/ig/Uploads/2007/Aug/20070816135739\_information -governance-standards-v2-web-070816.pdf

At the time of writing the Standards are under review.

The policy also draws on the NHSS Information Assurance Strategy.

http://www.sehd.scot.nhs.uk/mels/CEL2011\_26.pdf

## 5. Information Governance Responsibilities

The Director of Finance and Corporate Resources has board-level responsibility for Information Governance and is responsible for this policy, its implementation and monitoring.

The original policy was agreed by the Board with amendments being authorised by the ICT Information Governance Group. Monitoring implementation of the policy will be delegated to the ICT Information Governance Group who will receive and monitor a bi-annual Information Governance Improvement Plan. An Information Governance report will be submitted to the Board annually through the Finance and Corporate Performance Committee. The day-to-day co-ordination of Information Governance issues will be delegated to the Information Governance Manager, reporting to the Head of IM&T. These arrangements will be set out in a Management Procedure (MP19) within the information security management system.

NES will maintain a suite of policies, procedures and guidance supporting the Information Governance agenda which will be subject to ongoing review and improvement. These documents will be considered as extensions to this policy.

All NES staff are responsible for complying with all information governance requirements relevant to their role. All NES staff will receive basic training to Foundation level in the NHS Scotland Information Governance Competency Framework.

Risk assessment, in conjunction with overall priority planning of organisational activity, will be undertaken to determine appropriate effective and proportionate information governance controls are in place. Information governance issues will be captured within the Corporate Risk Register and the related reporting framework.

## 6. Confidentiality

With regard to privacy and confidentiality, NES will ensure compliance with the Data Protection Act 1998 (see below), The Human Rights Act 1998, the NHS Code of Practice on Confidentiality, the common law duty of confidentiality, NES’ duty of care and the Freedom of Information (Scotland) Act 2002 (see below).

The responsibilities of all staff for Confidentiality will be set out in their employment contracts.

The rights of staff to report legitimate concerns will be protected in line with the

Whistleblowing Policy within NHS Education for Scotland

http://intranet.nes.scot.nhs.uk/policies/HR/documents/Whistleblowing-Policy.doc

Responsibilities for Confidentiality will also form part of all contractual relationships with external organisations and relevant staff and stakeholders will be made aware of confidentiality requirements.

All those on whom NES holds personal information will be made aware of the uses to which the information may be used.

Incidents involving breaches of confidentiality and information security will be reported to the Information Governance Manager and a summary of incidents included within the annual IG report.

**7. Recording of Meetings**

The term ‘recording’ covers any type of audio and video recording device, including personally owned equipment. No recording of any meeting may be made without the express agreement of all participants at the meeting. Transcripts and a copy of the recording will be made available unless agreed otherwise.

Covert recording of a meeting would be illegal under the terms of the EU General Data Protection Regulation 2016 and the Regulation of Investigatory Powers (Scotland) Act.

Furthermore, any such recording would breach the principles of dignity and respect, and will be considered to be of a serious and unacceptable nature that is likely to result in disciplinary procedures.

## 8. Freedom of Information

The Freedom of Information Act (Scotland) 2002 enables any person to obtain information held by Scottish public authorities, including NES. This is a legal right and will ensure that all people swiftly receive information to which they are entitled. NES will seek to be as open as possible, both in pro-actively providing information to the wider community and in responding positively to requests for information. As well as meeting our statutory responsibilities, NES considers openness a vital component of our commitment to Patient Focus and Public Involvement (PFPI). The Information Governance Manager, as FOI lead, co-ordinates mechanisms to ensure NES’ statutory obligations are met.

(See Freedom of Information Procedure MP20, Media Communications Protocol and Access to Information policy.)

http://intranet.nes.scot.nhs.uk/policies/communications/documents/MediaCommunicationsPro tocol.DOC http://intranet.nes.scot.nhs.uk/policies/communications/documents/AccesstoInformationMerge dFinal.pdf

## 9. Records Management

NES recognises effective records management as being a key component of Information Governance and of our accountability and efficient service delivery. NES also acknowledges its statutory responsibilities under the Public Records (Scotland) Act 2011. Compliance with the NES Records Management policy is the

responsibility of all staff and should be embedded within all business processes. Appropriate guidance, practical support and training will be provided.

NES will manage the closure, retention and disposal of records, regardless of format, with reference to NHS Scotland guidance, such as the *Records Management: NHS*

*Code of Practice (Scotland)* http://www.scotland.gov.uk/Publications/2012/01/10143104/0

NES will work towards the standards of records management set out in the International Standard ISO15489.

(See Records Management Policy.)

http://intranet.nes.scot.nhs.uk/information\_governance/documents/RMP001NESRecordsMan agementPolicy.doc

## 10. Patient Records and Caldicott

As a Special Board without direct healthcare responsibilities, NES does not hold patient records. Where personal data on patients are incidentally captured, for example in evidence of health practitioner training, patient consent will be obtained and information will be held in line with the Data Protection policies of the relevant board or practice.

A NES clinical director will be designated as Caldicott Guardian and NES will observe the Caldicott principles where applicable.

## 11. Data Protection

NES holds personal data relating to health practitioners receiving training, education or appraisal, and relating to NES employees. NES fully adheres to the Principles of Data Protection as set out in the Data Protection Act 1998. NES will:

* observe conditions regarding the fair collection and use of information *(as defined under the 1st Principle)*
* meet its legal obligations to specify the purposes for which information is used *(as defined under the 2nd Principle)*
* collect and process appropriate information, and only to the extent that it is needed to fulfil legitimate operational needs or to comply with any legal requirements *(as defined under the 3rd Principle)*
* ensure the quality of information used *(as defined under 4th Principle)*
* apply retention policies to determine the length of time information is held *(as defined under the 5th Principle)*
* ensure that the rights of people about whom information is held can be fully exercised under the Act, including the rights to be informed that processing is being undertaken; the right of access to one’s own personal information; the right to prevent processing in certain circumstances and; the right to correct, rectify, block or erase information which is inaccurate. *(as defined under the 6th Principle)*
* take appropriate technical and organisational security measures to safeguard personal information *(as defined under the 7th Principle)*
* ensure that personal information is not transferred outside the European Economic Area without suitable safeguards *(as defined under the 8th*

*Principle*)

The Information Governance Manager fulfils the role of nominated Data Protection Officer, and will ensure that a full, correct and up-to-date notification is lodged in its name with the Information Commissioner as required by the Data Protection Act 1998 (see MEL(17)2000). This Officer’s advice will be sought when any new information system is being designed to ensure the system’s compliance with Data Protection requirements.

Individuals on whom NES holds personal data will be informed of their rights in relation to the use of their personal data. All contractual arrangements will include the appropriate requirements for confidentiality, data protection, freedom of information and information security.

(See Data Protection Procedure MP19)

## 12. Information Management

All NES’ major information assets will be accounted for in an Information Asset Register and have a nominated owner to ensure appropriate protection is maintained. Stakeholders will be involved in the development of information systems and information management arrangements will link effectively to educational and research governance arrangements.

## 13. Information Security

NES will maintain an Information Security Policy. The Information Governance Manager will fulfil the role of Information Security Officer, monitoring and advising on corporate information security arrangements NES will establish and maintain policies for effective and secure management of its information assets and resources in line with national policy and advice, for example as set out in NHS HDL (2006) 41, seeking compliance with International Standard ISO27001.

NES will maintain an Information Asset Register, assigning ownership of each major information/data set, its business justification and access restrictions.

All NES staff will have defined and documented information access rights and their responsibilities and business requirements for access control will be defined and documented. NES will have procedures to prevent unauthorised access, damage or interference to business premises and information. NES will follow standards to reduce the risks of human error, theft, fraud or misuse of information or facilities.

Where appropriate, independent audits will be undertaken to assess information security arrangements. NES’s incident reporting system will be used to report, monitor and investigate breaches of confidentiality and security. The availability of information systems will be preserved through the operation of clearly defined backup procedures and business continuity plans.

All computers, network communications and operations owned or used by NES will be managed, operated and maintained in a secure manner and to recognised security standards. All responsibilities for operational procedures are documented and all alterations to procedures will be subject for formal change control procedures. Any new information system developments will be developed and implemented in a secure manner to preserve the confidentiality, integrity and availability of NES systems.

In order to measure the impact of NES Information Governance Policy and associated procedures, staff will report to the Information Governance Manager any incident that places patient confidentiality or the confidentiality, security, integrity or availability of NES information at risk.

All NES equipment containing information storage media will be checked to ensure that any sensitive data and licensed software have been removed or overwritten prior to disposal. Where information is passed to other organisations, this will be done securely.

(See Information Security Policy IGP004)

## 14. Data Quality

As NES does not deal directly with patient clinical data, we are not subject to the clinical data quality standards and clinical coding issues which apply to other NHS Boards. However, NES recognises that high quality data is critical to accurate decision making, sound educational and research governance and accountability. NES will take proportionate measures to ensure the quality of business critical data.

NES will proactively identify its critical datasets which will be managed to the relevant data standards. These will have system audit trails, where appropriate linking data entered to specific individuals responsible for that data.

Internal and external audit and other quality assurance review processes will examine and underpin data quality in these critical areas. Where possible and proportionate, information quality will be assured at the point of collection.

Senior managers are expected to take ownership of and seek to improve the quality of data within their services. Internal and external audit will provide an independent check for data quality.

Relevant data quality standards and checks will, where relevant, form part of rolespecific training in NES.

## 15. Breaches of the policy

Intentional or negligent breaches of the Information Governance Policy and associated procedures will be considered to fall within the NES Disciplinary Policy and Procedures. In significant cases this may result in disciplinary action up to dismissal, and civil or criminal action where appropriate.

http://intranet.nes.scot.nhs.uk/documents/publications/classh/Disciplinary-policy-020211.doc

## 16. Normative documents

|  |  |
| --- | --- |
| International Standards Organisation  | ISO27000 Information Security Standards  |
| International Standards Organisation  | ISO15489 Records Management Standards  |
| NHS Education for Scotland  | *Information Governance in NHS Scotland – A Competency Framework* 2nd edition http://www.nes.scot.nhs.uk/media/584116/information\_govern ance\_in\_nhsscotland\_competency\_framework.pdf  |
| NHS National Services Scotland  | *Information Governance Standards. 2007* http://www.elib.scot.nhs.uk/SharedSpace/ig/Uploads/2007/Aug/2007 0816135739\_information-governance-standards-v2-web-070816.pdf [NOTE The Standards are under review at the time of writing.]  |
|   | Computer Misuse Act 1990 http://www.opsi.gov.uk/acts/acts1990/Ukpga\_19900018\_en\_1.htm  |
|   | Environmental Information (Scotland) Regulations 2004 http://www.legislation.gov.uk/ssi/2004/520/contents/made  |
|   | Freedom of Information (Scotland) Act 2002 http://www.opsi.gov.uk/legislation/scotland/acts2002/20020013.htm  |
|   | NHS Education for Scotland Order 2002 http://www.opsi.gov.uk/legislation/scotland/ssi2002/20020103.htm  |
|   | Data Protection Act 1998 http://www.opsi.gov.uk/acts/acts1998/19980029.htm  |
|   | Public Records (Scotland) Act 2011 www.legislation.gov.uk/asp/2011/12/contents/enacted  |
| Scottish Government Health Directorate  |  *Records Management Code of Practice (2012 edition)*  http://www.scotland.gov.uk/Publications/2012/01/10143104/0  |
| Scottish Government Health Directorate  | NHS Scotland Code of Practice on Protecting Patient Confidentiality 2012 http://www.knowledge.scot.nhs.uk/media/CLT/ResourceUploads/401 1563/Revised%20Code%20of%20Confidentiality%20-%20Final.pdf  |
| Scottish Government Health Directorate  | NHS IT Security Manual http://www.sehd.scot.nhs.uk/mels/HDL2006\_41.pdf  |
| Scottish Government Health Directorate  | Caldicott Guardians Manual (Scottish) 2011 http://www.scotland.gov.uk/Publications/2011/01/31115153/0  |

|  |  |
| --- | --- |
|  | **Document control**  |
| **Version**  | 2.1 Updated version  |
| **Title**  | NES Information Governance Policy  |
| **Summary**  | A policy document to set high-level standards for information governance within NHS Education for Scotland.  |
| **Date**  | August 2016 |
| **Author**  | Information Governance Manager (Frank Rankin)  |
| **Owner**  | Director of Finance and Corporate Resources (Caroline Lamb)  |
| **Document No.**  | IGP001 v 2.1 |
| **Document location:**  | Sharepoint DG/IG/IG policies |

|  |  |
| --- | --- |
|  | **Authorisation**  |
| **Approved by**  | Information Governance Group, Staff Governance Group  |
| **Date of approval**  | August 2013, January 2014  |
| **Date of Issue**  | Aug 2016 |
| **Supercedes**  | Version 2.0 of Feb 2014  |
| **Date for review:**  | Jan 2017  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Version history**  |  |
| **Date**  | **Version**  | **Status/ Summary of changes**  | **Author**  |
| December 2006  | 0.1  | Initial draft for internal review by Planning & Information Directorate  | Frank Rankin  |
| January 2007  | 0.2  | Revised draft for approval by Director  | Frank Rankin  |
| January 2007  | 0.3  | Incorporating comments from DC, CC  | Frank Rankin  |
| February 2007  | 0.4  | Incorporating comments from NSS. For Presentation to Business Group.  | Frank Rankin  |
| 20 February 2007  | 1.0  | Final version as approved by Business Group.  | Frank Rankin  |
| December 2010  | 1.1  | Incorporating minor updates to reflect management and regulatory framework changes  | Frank Rankin  |
| August 2013  | 1.2  | Updated to reflect new policy frameworks and submitted to Information Governance Group.  | Frank Rankin  |
| Sep 2013  | 1.3  | As approved by IGG for submission to PF and consultation  | Frank Rankin  |
| February 2014  | 2.0  | As approved by Staff Governance Committee  | Frank Rankin  |
| August 2016 | 2.1 | Incorporating meeting recordings text as agreed by SGC | Frank Rankin |