NIGALA
NI Guardian Ad Litem Agency
a voice for children

Information Governance Policy

Table of Contents

1 Introduction

1.1 Information governance (IG) describes the approach within which accountability, standards, policies and procedures are developed, implemented and maintained to ensure that all types of information are processed appropriately, securely and in line with current legislation. It has four fundamental aims:

- to support the provision of a high quality service by promoting the effective and appropriate use of information
- to encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources
- to provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards
- to enable organisations to understand their own performance and manage improvement in a systematic and effective way

1.2 Information held by NIGALA represents one of their most valuable assets, and core to most of the services delivered to their service users, business partners and customers. It is therefore essential that all information is managed effectively within a robust framework, in accordance with best practice and the legislative framework which includes:

- Data Protection Act 1998
- General Data Protection Regulations
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Public Records Act (Northern Ireland) 1923
- Disposal of Documents Order 1925
- Re-Use of Public Sector Information Regulation 2005
- Access to Health Records (Northern Ireland) 1923
- Human Rights Act 1998
- Audit & Internal Control Act 1987
- Copyright, Designs and Patents Act 1988
- Copyright (Computer Programs) Regulations 1992
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- Equality Act 2010
- Health and Social Care Act
- Public Interest Disclosure Act 1998
- The Investigatory Powers Act 2016
- Guidance from the Information Commissioners Office
- The Department of Health (DoH) Good Management, Good Records
- Information Management Controls Assurance Standard (IMCAS) issued by DoH

1.3 Having accurate relevant information available at the time and place where it is needed, is critical in all areas of business and plays a key part in corporate governance as well as risk, planning and performance management.

1.4 The Northern Ireland Guardian AD Litem Agency (NIGALA) carries a legal responsibility for the appropriate processing and protecting information of many

types. This includes information which contains personal details of patients/clients, their families or staff.

1.5 This policy also recognises the need to share identifiable personal information with other health organisations and agencies in a controlled manner consistent with the interests of the individual and, in some circumstances, in the public interest.

1.6 Some information may be non-confidential and is for the benefit of the general public. Examples include information about services, annual report and business plans. NIGALA and its employees share responsibility for ensuring that this type of information is accurate, up to date and easily accessible to the public.

1.7 Although the majority of information about NIGALA should be open for public scrutiny, it is acknowledged that some information, which is commercially sensitive, may need to be safeguarded.

1.8 The associated policies underpinning Information Governance for NIGALA are included in the Appendices.

2 Purpose

The IG requirements set out within this policy and subsequent policies and procedures are intended to:

- outline the approach to fulfilling IG responsibilities;
- ensure compliance with legal and regulatory framework is maintained;
- establish a robust framework for preserving the confidentiality, integrity, security and accessibility of data, systems and information;
- give assurance that information is processed legally, securely, efficiently and effectively

2.1 This policy acts as an overall umbrella policy that sets out the approach to be adopted for the processing of information, sitting over the other policies relating to each aspect of Information Governance.

2.2 The IG requirements set out within this policy and subsequent policies and procedures are intended to ensure that there is a robust framework concerning the obtaining, recording, holding, using, sharing and destruction of all data and records held or used and ensuring that relevant information is available where and when it is needed.

3 Scope

3.1 The scope of this policy is to support the protection, control and management of information assets. The policy covers all information within NIGALA and is concerned with all information systems, electronic and non-electronic. It applies to all directorates, services and departments, all permanent and temporary staff, all agency staff, and as appropriate to contractors and third party service providers acting on behalf of the organisation, including self-employed Guardian Ad Litems.

3.2 IG covers all information held, and all information systems used to hold that information. This includes, but is not necessarily limited to:

- stored on computers
- transmitted across internal and public networks such as email or Intranet/Internet
- stored within databases
- printed or handwritten on paper, whiteboards (etc.)
- sent by facsimile (fax), telex or other communications method
- stored on removable media such as CDs, hard disks, pen drives, tapes and other similar media
- stored on fixed media such as hard drives and disk subsystems
- held on film or microfiche
- paper and electronic structured records systems
- information recording and processing systems whether paper electronic video or audio records
- presented on slides, overhead projectors, using visual and audio media
- spoken during telephone calls and meetings or conveyed by any other method

3.3 This policy covers all forms of information held, including (but not limited to):

- Information about members of the public
- Non- employees on organisational premises
- Staff and Personal information
- Organisational, business and operational information

3.4 This policy covers all information systems purchased, developed and managed by/or on behalf of NIGALA and any individual directly employed or otherwise used by NIGALA

4 Policy

There are seven key, interlinked strands to this policy

- Openness.
- Legal compliance.
- Information security.
- Quality Assurance.
- Information Risk Management.
- Records Management
- Training and Awareness.

4.1 Openness

This policy recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. Confidential information will be defined and where appropriate kept confidential, underpinning the principles and the regulations outlined in the Data Protection Regulations[1]

Non-confidential information will be available to the public through a variety of means, one of which will be the provisions of the Freedom of Information Act 2000.

[1] The Data Protection Regulations are The Data Protection Act (1998) and the EU General Data Protection Regulations

Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.

The availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience. This is supported by appropriate business continuity plans.

The NIGALA will:

- establish procedures and arrangements for handling queries from service users and members of the public
- undertake or commission regular assessments and audits of IG policies and arrangements
- ensure that non-confidential information about the organisation and its services is readily and easily available through a variety of media, in line with the ICO's model publication scheme
- proactively use information to support care, in compliance with the legislation and codes of practice issued by relevant regulators and DoH best Practice

4.2 Legal Compliance

All identifiable personal information is classified as confidential, except where national policy on accountability and openness requires otherwise.

The NIGALA will:

- establish and maintain policies and procedures to ensure compliance with Data Protection Regulations, Human Rights Act 1998, the common law duty of confidentiality, Environmental Information Regulations 2004, and the Freedom of Information Act 2000
- treat all identifiable personal information as confidential
- develop and maintain the appropriate registers and systems to permit its functions as a data controller, and to act as a shared controller where this is required
- establish and maintain policies and procedures for the controlled and appropriate sharing of service user information, taking account of relevant legislation

4.3 Information Security

NIGALA is dedicated to the secure management and use of information held, and compliance with the legislation and codes of practice issued by relevant regulators and the DoH in respect to information security.

The NIGALA will:

- establish and maintain an Information Security Policy along with respective procedures for effective policing and secure management of all information assets and resources
- establish and maintain appropriate incident reporting procedures to report, monitor and investigate all instances actual and/or potential along with any reported breaches of confidentiality and security
- undertake and/or commission audits to assess Information and ICT Security arrangements

- promote effective confidentiality and security practice to ensure all permanent/temporary, contracted staff and third party associates adhere to this via appropriate laid down policy procedures, training and information awareness schemes/documentation

4.4 Information Quality Assurance

Data can be defined as a collection of text, figures or statistics which can be translated and processed into information. Information quality is a measurement of the robustness and usefulness of that data for its intended purpose. Information quality is fundamental to providing sound information to support business decision making processes and underpinning all activities and actions.

The NIGALA will:

- establish and maintain policies for information quality assurance and the effective management of records
- ensure that information it holds, through business arrangements, is of the highest quality in terms of completeness, accuracy, relevance, accessibility, timeliness and intelligibility
- ensure that managers are required to take ownership of, and seek to improve the quality of information within their functional areas and that information quality is assured at the point of collection
- undertake or commission regular assessments and audits of its information quality and records management arrangements
- ensure that data standards are set through clear and consistent definition of data items, in accordance with quality standards
- promote information quality and effective records management through policies, staff awareness and training
- report and act upon incidences of known or suspected poor data quality

4.5 Information Risk Management

All information assets and information flows should be risk assessed to determine appropriate, effective and affordable IG controls are in place

Risk assessment in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate, cost-effective IG controls are in place.

4.6 Records Management

Records management is a discipline to manage the creation, control, distribution, retention, storage and disposal of records. The underlying principle is to ensure that a record is managed through its life cycle from creation or receipt, through maintenance and use to disposal.

The NIGALA will:

- establish and maintain policies for effective records management
- promote records management through policies, procedures and training

4.7 Training

Awareness and understanding of all staff, with regard to their responsibilities, will be routinely assessed, recorded and appropriate training and awareness provided.

The NIGALA will ensure that:

- all staff complete mandatory training at induction, and on a 2 yearly cycle thereafter
- All staff have access to relevant IG policies and procedures

5 Responsibilities

5.1 The **Board** has overall responsibility to ensure compliance in all areas of information governance.

5.2 The **Chief Executive** has ultimate responsibility for the delivery of this policy and associated policies and procedures.

5.3 The **Personal Data Guardian (PDG)** is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing.

5.4 The **Senior Information Risk Officer (SIRO)** is an executive who has responsibility to ensure compliance with legislation through the development and monitoring of policy and codes of practice, and the appointment of Information Asset Owners (IAOs).

5.5 **IAOs** are senior individuals involved in running the relevant business area within each organisation. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and the use of those assets. The IAO should:

- know who has access to the asset and why
- ensure access is monitored and auditable
- understand, measure and address risks to the asset and provide assurance to the SIRO

5.6 **Information Asset Administrators (IAAs)** ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date. The IAA will be a member of Operational staff responsible for one or more information assets as nominated by the IAO for the area of responsibility.

5.7 The **Head of Corporate Services** is the designated **Information Governance Lead (IGL)** Key responsibilities include:

- ensuring there is senior level awareness and support for IG
- providing direction in formulating, establishing and promoting IG in the organisation
- drafting ,reviewing, revising, distributing and implementing IG policies

- monitoring and reporting on performance
- ensuring completion of Department of Health assurances, audit reports and improvement action plans are prepared for approval
- developing appropriate training for staff

5.8 **Assistant Directors** are responsible individually and collectively for the application of the Information Governance suite of policies within their Groups.

5.9 **Managers** are responsible for ensuring that this policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance with the standards set out in the documents that make up the IG Framework.

5.10 **Managers** must also ensure that this policy and its supporting standards and guidelines are conveyed to their staff and any third party contractor working in the area and that there is on-going compliance with the standards set out in the documents that make up the IG Framework. They must also ensure that staff are adequately trained and apply the appropriate guidelines.

5.11 All **Staff** members, whether permanent, temporary or agency are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

5.12 **Information Governance Committee**

The NIGALA operates an internal committee the **Information Governance Committee**. This committee is a committee of the board. It is chaired by a board member and members include the Chief Executive, Head of Corporate Services, Records Management Officer and Guardians.

The group will seek assurances and provide scrutiny on:

- The development of an information governance culture within NIGALA.
- The development of a comprehensive Corporate Information Asset Register
- develop policies and procedures to assist in the protection and safe use of information within NIGALA
- The compliance within the organisation of all aspects of the IG Strategy
- The review of policies in relation to IG on a regular basis
- The development of support arrangements and provision to staff of appropriate training and support to enable them to discharge their responsibilities to consistently high standards
- The development action plans to ensure on-going improvements in the management of IG within NIGALA
- The maintenance an overview of incidents affecting IG and security
- Identification of training and development requirements for staff within NIGALA in respect of IG

5.13 The **Business Service Organisation** provides administrative support and professional advice to NIGALA on IG issues and developments. The services of the Business Services Organisation are set out in an annual Service Level Agreement. In providing its services to NIGALA the Business Services Organisation is considered a Data Processor as set out under GDPR. Services include the provision of a **Data Protection Officer** under requirements as set out by the GDPR.

6 Performance and Monitoring Compliance

The effectiveness of this policy will be assessed on a number of criteria:

- compliance with legislation
- the management (including frequency) of data breaches including inappropriate release of information, including near misses
- the retention, disposal and destruction of records in accordance with GMGR
- staff training records

7 Non-Compliance

A failure to adhere to the policy and its associated procedures/guidelines may result in disciplinary action and /or dismissal. Any breach of policy will be investigated and disciplinary action may be taken regardless of whether organisational equipment or facilities are used for the purpose of committing the breach. In relation to the use of ICT Equipment including the use of the Internet and Email, staff should be aware that they might be personally liable to prosecution and open to claims for damages if their actions are found to be in breach of the law.

Serious breaches may be reported to the PSNI, ICO or other public authority for further investigation.

8 Review

This policy and all associated documents within the Information Governance Framework will be reviewed no later than 2 years from approval, to ensure their continued relevance to the effective management of Information Governance within NIGALA.

9 Equality Statement

In accordance with the NIGALA`S Equal Opportunities policy, this policy and associated policies will not discriminate, either directly or indirectly, on the grounds of gender, race, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, background or any other personal characteristic.

APPENDICES – Supporting policies

APPENDIX 1

Data Protection and Confidentiality

Contents

1. Introduction

1.1 Background

The Northern Ireland Guardian Ad Litem Agency (NIGALA) needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include children employees (present, past and prospective), suppliers and other business contacts. In addition, we may be required by law to process and share personal information with other organisations (including, but not limited to, police, regulatory and health and social care bodies).

As a public body, NIGALA has a statutory duty to safeguard the information it holds, from whatever source, which is not in the public domain. The lawful and proper treatment of personal information by NIGALA is extremely important to the success of our business and in order to maintain the confidence of our service users and employees.

1.2 Data Protection Principles

NIGALA its staff and others who process personal information on its behalf must ensure that they follow the principles set out within Article 5 of the GDPR, namely that personal information will be:

(a) processed lawfully, fairly and in a transparent manner;
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
(d) accurate and, where necessary, kept up to date;
(e) 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;
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

1.3 Supporting Legislation

This policy has been written to support staff in compliance with legal requirements and best practice guidance as set out in the NIGALA's overarching Information Governance Policy.

2. Purpose

The purpose of this policy is to lay down the principles that must be observed by anyone who works for, or on behalf of, NIGALA and have access to personal information.

This policy aims to clarify how and, when personal information may be shared, the need to make individuals aware of the ways in which their information might be used.

3. Scope

The scope of this policy is to support the protection, control and management of personal information. The policy will cover all information within NIGALA and is concerned with all information systems, electronic and non-electronic information. It applies to all directorates, services and departments, all permanent and temporary staff, all agency staff, and as appropriate to contractors and third party service providers acting on behalf of NIGALA, including Self Employed Guardians.

This includes, but is not necessarily limited to information:

- stored on computers, paper and electronic structured records systems
- transmitted across internal and public networks such as email or Intranet/Internet
- stored within databases
- printed or handwritten
- stored on removable media such as CDs, hard disks, pen drives, tapes and other similar media
- stored on fixed media such as hard drives and disk subsystems
- held on film or microfiche
- information recording and processing systems whether paper electronic video or audio records
- presented on slides, overhead projectors, using visual and audio media
- spoken during telephone calls and meetings or conveyed by any other method

This policy covers all forms of information held, including (but not limited to):

- Information about members of the public
- Non- employees on organizational premises
- Staff and Personal information
- Organizational, business and operational information

This policy covers all information systems purchased, developed and managed by/or on behalf of, NIGALA and any individual directly employed or otherwise used by NIGALA

4. Definitions

4.1 Personal Information

The term ’personal information’ applies to any data relating to an identified or identifiable natural person. It relates to both electronic and manual information held in any format.

4.2 Special categories of personal information

Article 9 of GDPR defines ‘special categories’ of personal information as information relating to:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic or biometric data for the purpose of uniquely identifying a natural person
- health (mental or physical)
- sexual life or sexual orientation

This policy informs the Information Governance Policy and should be read alongside the ICT Security Policy, which deal with the security of information held by NIGALA and gives important guidance in this respect.

4.3 Data Controller

The ‘data controller’ is defined as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

4.4 Data Processor

A ‘data processor’ is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller.

5. Objectives

NIGALA will apply the above principles to the management of all personal information by adopting the following policy objectives:

5.1 Privacy by design

NIGALA will apply 'privacy by design' when developing and managing information systems containing personal information by

- Using proportionate privacy impact assessment to identify and mitigate data protection risks at an early stage of project and process design for all new or updated systems and processes
- Adopt data minimisation: NIGALA will collect, disclose and retain the minimum personal information for the minimum time necessary for the purpose(s) that it is being processed
- Anonymise personal data wherever necessary and appropriate, for instance when using it for statistical purposes

5.2 Fair and Lawful Processing

NIGALA will:

- Only collect and use personal information to the extent that it is needed to fulfil operational or legal requirements, and in accordance with the conditions set down under GDPR, namely:
    - Consent of the Data subject
    - To perform in terms of a contract
    - To comply with a legal obligation
    - To protect a data subject's vital interests
    - If it is in the public interest
- Provide transparent information on how personal information will be processed by way of 'fair processing notice', which will detail:
    - What information is needed
    - Why this information is needed
    - The purpose(s) that this information will be used for
    - How long this information will be kept for
- Ensure that personal information is collected for specific purpose(s), and will not be reused for a different purpose that the individual did not agree to or expect
- Ensure the quality of personal information processed

5.3 Disclosure of Personal Information

Strict conditions apply to the disclosure of personal information both internally and externally. NIGALA will not disclose personal information to any third party unless it is lawful to do so. In certain circumstances, information relating to staff acting in a business capacity may be made available provided:

- we have the statutory power or are required by law to do so; or
- the information is clearly not intrusive in nature; or
- the individual has consented to the disclosure; or
- the information is in a form that does not identify the individual

5.4 Right of Access

GDPR gives any individual who has personal data kept about them by NIGALA the right to request in writing a copy of the information held relating to them. NIGALA will ensure that an applicant receives access within a calendar month, unless there is a valid reason for delay or an exemption is applicable. The Business Services Organisation handles information requests on behalf of NIGALA and provides professional advice in regard to Information Governance.

5.5 Safeguarding Information

NIGALA will ensure appropriate technical and organisational security measures are in place to safeguard personal information so as to prevent loss, destruction or unauthorised disclosure. For further information and guidance, please refer to the following policies:

- Information Risk Policy – Appendix 3
- Information Security Policy – Appendix 5

5.6 Retention and Disposal

GDPR places an obligation on NIGALA not to keep personal information for longer than is required for the purpose(s) for which it was collected. Personal information will be disposed of by means that protect the rights of those individuals, and as such NIGALA will:

- Apply retention policies to all personal information
- Destroy information no longer required in a secure manner
- Transfer the information, by arrangement, to the Public Records Office of Northern Ireland (PRONI) where deemed appropriate

5.7 Uphold Individual's Rights

NIGALA will ensure that the rights of the individual under GDPR are upheld, where applicable, namely:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The rights in relation to automated decision making and profiling.

6. Responsibilities

5.1 The **Board** has overall responsibility to ensure compliance in all areas of information governance.

5.2 The **Chief Executive** has ultimate responsibility for the delivery of this policy and subsequent policies and procedures.

5.3 The **Personal Data Guardian (PDG)** is a senior person responsible for protecting the confidentiality of personal information.

5.4 The **Data Protection Officer (DPO) at BSO** is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements

5.5 **Assistant Directors** are responsible individually and collectively for the application of the Information Governance suite of policies within their groups. Directorates.

5.6 The **Head of Corporate Services** is responsible for ensuring compliance with FOI requirements.

5.7 **Managers** are responsible for ensuring that this policy and its supporting standards and guidelines are built into local processes.

5.8 All **Staff** members, whether permanent, temporary or agency are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis. Staff are expected to:

- Familiarize themselves with, and abide by, the principles set out within this policy
- Understand how to safeguard personal information

5.9 Any **third parties** who are users of personal information processed by NIGALA will be required to confirm and demonstrate that they will abide by the requirements of GDPR.

5.10 The **Business Services Organisation** handles information requests on behalf of NIGALA and provides professional advice in regard to Information Governance. In doing so the Business Services Organisation is considered a Data Processor as set out under GDPR.

6 Performance and Monitoring Compliance

6.1 The effectiveness of this policy will be assessed on a number of criteria:

- Nomination of an individual or individual with specific responsibility for data protection within NIGALA

- compliance with legislation in respect of GDPR;
- the management of data breaches, including near misses;
- the retention and disposal of records in accordance with GMGR;
- performance against agreed standards on an annual basis;

7 Non-Compliance

A failure to adhere to **Data Protection and Confidentiality** and its associated procedures/guidelines may result in disciplinary action and /or dismissal. Any breach of policy will be investigated and disciplinary action may be taken regardless of whether organisational equipment or facilities are used for the purpose of committing the breach. In relation to the use of ICT Equipment including the use of the Internet and Email, staff should be aware that they might be personally liable to prosecution and open to claims for damages if their actions are found to be in breach of the law. Serious breaches may be reported to the PSNI, ICO or other public authority for further investigation.

Appendix 2 Data Protection Impact Assessments

Contents

7. Introduction

A Data Protection Impact Assessment (DPIA) is an assessment of the impact of envisaged data processing operations on the protection of personal data, and particularly an assessment of the likelihood and severity of risks for the rights and freedoms of individuals resulting from this operation.

Under Article 35 of the General Data Protection Regulations (GDPR), data controllers will be legally required to undertake DPIAs prior to data processing which is *"likely to result in a high risk to the rights and freedoms of natural persons*".

8. Benefits

A DPIA will assist stakeholders in a structured way to identify, categorise and mitigate privacy risks when processing personal data. In addition to the mandatory protection of personal data, a robust DPIA process results in the following:

- Preventing costly adjustments in processes or system redesign by mitigating privacy and data protection risks
- Prevention of discontinuation of a project by early understanding the major risks
- Improving the quality of personal data
- Improving service and operation processes
- Improving decision-making regarding data protection
- Raising privacy awareness
- Improving the feasibility of a project
- Improving communication about privacy and the protection of personal data

9. Purpose

The purpose of this document is to provide guidance on how to assess whether a DPIA is required, and subsequently how to undertake and document a DPIA.

Specifically, this document is designed to assist in the identification and assessment of risks to personal data, as well as to assist in the documentation of envisaged safeguards and control measures in proportion to the risks identified. As such, this document shall also be considered integral to the Northern Ireland Guardian Ad Litem Agency (NIGALA) wider risk management process.

10. Scope

In general, data protection impact assessments are appropriate for projects where one or more of the following applies:

- personal information will be collected and processed for the first time;
- personal information will be shared with people or organisations that previously did not have access to it;
- change of use of existing personal data;
- the use of new technology that processes personal data (e.g. biometrics);
- existing personal data will be used to reach decisions as part of an automated process;
- it might reasonably be expected that an individual may find any aspect of the project intrusive or the data involved private[2];
- processing on a large scale of special categories of data referred to in Article 9(1) of GDPR or of personal data relating to criminal convictions and offences referred to in Article 10 of GDPR;
- datasets that have been matched or combined, which therefore has the potential to identify individuals from previously anonymised / pseudonomised information;
- when the processing in itself 'prevents data subjects from exercising a right or using a service or a contract'

10.1 Format

While GDPR does not prescribe any process or format, a DPIA will contain at least the following:

- a description of the envisaged processing operations and the purposes of the processing, including the legal basis for such;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects that are likely to result from the processing; and,
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and demonstrate compliance with the GDPR

10.2 When to perform a DPIA

In the case of the development of a new application or system, a DPIA exercise must be carried out from the start of the design and implementation phase, prior to the processing of any personal information. This enables a 'Privacy by Design' approach guaranteeing that potential risks are identified and that appropriate controls can then be incorporated.

[2] In the context of this document, the definition of privacy includes the fundamental rights defined in Articles 7 and 8 of the European Union Charter of Human Rights, the right to privacy and the right to the protection of personal data.

With already existing applications, systems or processes the following criteria should also be considered:

- significant changes that expand beyond the original purpose(s);
- new types of information processed are introduced;
- unexpected personal data breach with significant impact, the occurrence of which hadn't been previously identified;
- a periodic or defined review is triggered;
- in response to significant internal or external stakeholder feedback or inquiry;
- if there are technological-related changes that may have data protection implications (e.g. cloud computing)

10.3 Consultation

Appropriate stakeholders must be involved within the development of a DPIA, in order to ensure all of the following aspects are adequately covered:

- Risk assessment
- IT architecture and system engineering
- Information security
- Privacy and data protection
- Organisational design
- Project management

As a minimum, this should include:

- the person(s) in charge of the application / system which is the target of the DPIA;
- person(s) in the design environment, with knowledge of the application / system in question;
- person(s) in the user environment;
- the Data Protection officer (DPO);

In the event that the results of the data protection impact assessment indicate a high level of risk prior to the identified controls being implemented, the GDPR requires that the supervisory authority[3] is consulted before any processing takes place.

11. Conducting the DPIA

11.1 Pre-Assessment

The objective of a pre-assessment questionnaire is to conduct an initial analysis of

[3] *The Information Commissioner's Office (ICO) is United Kingdom's supervisory authority*

the system / application / process in question at a 'high level', using a number of criteria to determine whether a full DPIA is required.

This initial questionnaire is set out within the DPIA Pre-Assessment Questionnaire (Appendix 1), and will include the following questions:

- The personal data involved
- Purpose
- Organisational structure / reporting
- Impact on rights / freedoms
- The nature of the applications / system
- Legal basis for processing

11.2 In-depth DPIA

If a determination is made that a more comprehensive DPIA is required, a separate Questionnaire (Appendix 2) will be completed. This will include detailed descriptions of:

- The use of personal data
- Identification, characterisation and description of systems/applications, including data flows
- Identification of relevant risks
- Risk Assessment
- Risk Management
- DPIA Final Report
- Management Approval
- Consultancy with the ICO, if appropriate
- Monitoring / Review

12. Responsibilities

6.1 **The NIGALA Board** has overall responsibility for effective risk management and this includes oversight of the management of information management within NIGALA for which the Chief Executive is accountable.

6.2 **The Head of Corporate Services** is responsible for ensuring that the policy is fully implemented in NIGALA and will provide an annual assurance to the Chief Executive Officer that all relevant DPIAs have been conducted on an annual basis.

6.3 **The Data Protection Officer at BSO** will:

- Assist in the production of pre-assessment and DPIA reports;
- Make recommendations and establish mechanisms for review of projects as appropriate

6.4 **All staff** members, whether permanent, temporary or agency are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis. Staff are expected to familiarise themselves with, and abide by, this policy. Specifically, all staff are responsible for:

- adhering to the requirements within this policy and relevant legislation;
- reporting any relevant incident in line with this policy;
- provision of information and/or reports as requested as part of an investigation;
- taking appropriate action to ensure incidents do not recur.

6.5 The **Business Services Organisation** provides support and professional advice to NIGALA on Information Governance. In doing so the Business Services Organisation is considered a Data Processor as set out under GDPR.

13. Non-Compliance

A failure to adhere to this policy and any associated procedures may result in disciplinary action. In relation to the use of ICT Equipment including the use of the Internet and Email, staff should be aware that they might be personally liable to prosecution if their actions are found to be in breach of the law. Serious breaches may be reported to the PSNI, ICO or other public authority for further investigation.

Appendix 3: Information Risk

Table of Contents

1 Introduction

1.1 Information is a vital asset, both in terms of the management of health and social care for individual service users and the efficient management of services and resources. It plays a key part in governance, service planning and performance management.

1.2 Information Risks are risks that relate to the loss, damage, or misuse of information or which threatens the confidentiality, integrity or availability of an information asset, especially information which is personal or confidential in nature.

1.3 Information risk is inherent in all administrative and business activities and everyone within the HSC continuously manages information risk. Information risks should be handled in a similar manner to other major risks such as financial, legal and reputational risks, and should not be seen as something that is the sole responsibility of Information Governance (IG) staff.

1.4 Information risk management is an essential component of information governance and is an integral part of continuous quality improvement. The aim of information risk management is to provide the means to identify, prioritise and manage the risks involved in all of the organisation's activities, and to embed this in a practical way into business processes and functions.

1.5 It is therefore of paramount importance to ensure that information risk is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

1.6 This policy and its associated sub policies and procedures define how information risk will be managed.

2 Purpose

2.1 The purpose of this document is to provide a risk management framework in which information risks are clearly recognised and the appropriate controls implemented in order to:

- protect the Northern Ireland Guardian Ad Litem Agency, it's staff and clients from information risks where the likelihood of occurrence and the consequences are significant
- provide a consistent risk management framework in which information risks will be identified, considered and addressed in key approval, review and control processes
- encourage pro-active rather than re-active risk management
- provide assistance to and improve the quality of decision making
- meet legal or statutory requirements
- assist in safeguarding information assets
- seek to minimise the risk of information governance (IG) incidents from occurring through the misuse of personal and/or sensitive data

3 Scope

3.1 This policy relates to the use of all organisation-owned information assets (both physical and system based), network applications, to all privately owned systems when connected directly or indirectly to the NIGALA network and to all organisation-owned and/or licensed or sanctioned software/data and equipment. This includes, but is not necessarily limited to:

- stored on computers
- transmitted across internal and public networks such as email or Intranet/Internet
- stored within databases
- printed or handwritten on paper, whiteboards (etc.)
- sent by facsimile (fax), telex or other communications method
- stored on removable media such as CDs, hard disks, pen drives, tapes and other similar media
- stored on fixed media such as hard drives and disk subsystems
- held on film or microfiche
- paper and electronic structured records systems
- information recording and processing systems whether paper electronic video or audio records
- presented on slides, overhead projectors, using visual and audio media
- spoken during telephone calls and meetings or conveyed by any other method

3.2 This policy covers all forms of information held by, including (but not limited to):

- Information about members of the public
- Non- employees on organisational premises
- Staff and Personal information
- Organisational, business and operational information

3.3 This policy covers all information systems purchased, developed and managed by/or on behalf of the NIGALA.

3.4 This policy applies to all directorates, services and departments, all permanent and temporary staff, all agency staff, and as appropriate to contractors and third party service providers acting on behalf of the NIGALA.

4 Responsibilities

4.1 The **Chief Executive is the Accountable Officer** and has overall responsibility for ensuring that information governance is applied throughout the organisation. He/she is responsible for ensuring that information risks are assessed and **managed to ensure information risk is reduced.**

4.3 The **Personal Data Guardian (PDG)** is responsible for:

- ensuring that the Information Risk policy is produced and kept up to date
- producing operational standards, procedures and guidance on Information Risk matters for approval by the Information Governance Management Committee (IGMC)

- co-ordinating Information Risk activities, particularly those related to shared information systems or ICT infrastructures
- liaising with external organisations on Information Risk matters
- reporting to the IGMC on matters relating to Information Risk
- take a lead on confidentiality issues, acting as a champion for data at Board level ensuring that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for all staff

4.5 The **Senior Information Risk Owner (SIRO)** will be responsible for

- coordinating the development and maintenance of information risk management strategies, policies, procedures and standards
- ensuring that the approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff
- providing a focal point for the resolution and/or discussion of information risk issues
- on-going development and day-to-day management of the Information Risk Management Programme for information privacy and security
- taking ownership of risk assessment processes for information risk, including the review of an annual information risk assessment to support and inform the statement of internal control
- ensuring that risks to IS are reduced to an acceptable level by applying counter measures identified following an assessment of the risk for each asset
- advising the Accountable Officer and the NIGALA Board on information risk management strategies and provide periodic reports and briefings on Programme progress
- ensuring that the Information Risk Management Policy supports the general risk management process

4.7 **Assistant Directors** are responsible for ensuring the local implementation of Information Governance and that they implement this and appropriate IG policies within their sphere of responsibility. This includes taking suitable management action should non-compliance arise.

4.8 **Managers** are held accountable for making sure that their staff are aware of their roles and responsibilities in relation to managing information risk. They in conjunction with the Corporate Service Manager will identify the level of training required for each member of staff and ensure that have time to carry out the appropriate level of training and have access to appropriate supervision and support.

4.9 **Information Asset Owners (IAOs)** are senior individuals who will:

- ensure that information risk assessments are performed quarterly on all information assets where they have been assigned ‘ownership’, following guidance from the SIRO on assessment method, format, content and frequency
- submit the information risk assessment results and associated risk management action plans to the SIRO for review, along with details of any assumptions or external dependencies. Mitigation plans shall include specific

actions with expected completion dates, as well as an account of residual risks
- ensure information risk management is embedded into the key controls and approval processes of all major business processes and functions

4.10 **Information Asset Administrators (IAAs)** works in conjunction with and on behalf of the IAOs to:
- ensure policies and procedures are followed
- recognise actual and potential security incidents
- consult with their IAO on incident management
- ensure that information asset registers are up to date

4.11 **The Head of Corporate Services** has responsibility for:
- operational management of IG and for the implementation and co-ordination of the IG work programme, although responsibility for specific requirements is devolved to specialist leads and service managers
- providing advice and guidance on creating and maintaining the information risk management framework
- informing the ICO of all Serious Adverse Incidents relating to information governance, and reporting to the Information Governance Management Committee (IGMC)
- ensuring the information risk register is regularly reviewed by the IGMC

4.12 It is the responsibility of all **employees, volunteers, contractors and subcontractors, including Self Employed Guardian Ad Litems,** to:
- ensure compliance with this and other information governance policies and procedures and must undertake annual training
- carry out their roles in accordance with this policy
- abide by the conditions detailed within this policy

4.13 The **Business Services Organisation** provides support and professional advice to NIGALA on Information Governance. In doing so the Business Services Organisation is considered a Data Processor as set out under GDPR.

5 Assessment of Information Risks

5.1 Information risk management is the process of identifying vulnerabilities and threats to information resources in achieving business objectives, and deciding what countermeasures, if any, to take based on the value of the information resource.

5.2 Identification and threat assessment of risks to information assets will be carried out in line with Risk Management policy and the Risk Register.

5.3 NIGALA will take all reasonable steps to protect data whose release or loss could cause:
- harm or distress to clients, patients or staff
- damage to reputation or financial loss
- major breakdown in information systems, information security or information integrity
- potential for an IG incident requiring investigation

5.4 BSO will maintain an Information Asset Register (IAR) for NIGALA which will be managed by each IAO for their area(s) of responsibility, in conjunction with the IAAs.

5.5 Each organisation will undertake an annual review of Information Flow Mapping and determine potential information risks regarding its data flows. The process will be managed by the Head of Corporate Services.

5.6 Risk Assessments will be conducted for all information systems and critical information assets. Information Risk Assessments should occur:

- within six months of issue of this policy, and on annually thereafter
- at the inception of new systems, applications, facilities (etc.) that may impact the assurance of information or information systems*
- before enhancements, upgrades and conversions*
- when HSCNI / Department of Health (DoH) policy or legislation requires risk determination
- when required by NIGALA Board

** Those containing or which involve personal information require a Data Protection Impact Assessment as a part of the development process.*

5.7 Risk must be assessed in terms of the general level of harm that could be reasonably caused if data were to become compromised or unavailable. The risk assessment should cover:

- the balance between level of risk, tolerance of risk and the effort being used to manage the risk
- identification of gaps between the current and target risk positions
- progress being made against agreed information risk priorities
- the effectiveness of the risk management controls including successes and failures

5.8 Information risk mitigation must be:

- commensurate with the level of risk
- kept simple so that it is manageable and can be communicated to staff
- supplemented with customised controls for specific high risk circumstances

5.9 All significant findings should be recorded and action plans prepared. These should be available for audit.

5.10 Risk Assessment tools and DPA Compliance Checklists will be made available by the Head of Corporate Services.

5.11 Action plans should be recorded at service level meetings where Information Governance is a standing item on the agenda.

6 Information Incident Management

6.1 Security breaches, information loss or unauthorised disclosure, and other risks associated with information management will be managed in line with the NIGALA`s s overall adverse incident reporting processes and template. All such incidents must be documented on an Adverse Incident Form, and could involve:

- loss of patient information
- loss of staff information
- loss of business information
- loss of hardware
- virus or malware attacks
- unauthorised access to information assets
- misuse of access privileges

7 Performance and Monitoring Compliance

7.1 Indicators that the policy is being enacted are:

- statutory reporting requirements are met
- assessments are completed
- no involvement of the ICO as a result of good practice

7.2 Indicators for Audit are:

- an identified IAO for each information asset
- an information asset register
- inclusion of information risks on risk registers
- number of information risks effectively mitigated and score reduced to lowest achievable

8 Non-Compliance

8.1 A failure to adhere to the policy and its associated procedures/guidelines may result in disciplinary action and /or dismissal. Any breach of policy will be investigated and disciplinary action may be taken regardless of whether organisational equipment or facilities are used for the purpose of committing the breach. In relation to the use of ICT Equipment including the use of the Internet and Email, staff should be aware that they might be personally liable to prosecution and open to claims for damages if their actions are found to be in breach of the law. Serious breaches may be reported to the PSNI, ICO or other public authority for further investigation.

Appendix 4 Freedom of Information

Contents

1. Introduction

The Freedom of Information Act 2000 (FOI) gives the public a general right of access to information held by a public authority, subject to certain conditions and exemptions. FOI promotes greater openness and accountability across the public sector, therefore facilitating a better understanding of how public bodies carry out their business and how they spend public money.

FOI places a statutory obligation the Northern Ireland Guardian Ad Litem Agency to publish details of all recorded information that it holds, except where an exemption applies. FOI is wholly retrospective and applies to all information held by public authorities regardless of its date.

The Environmental Information Regulations 2004 (EIR) gives the right to access 'environmental information' held by public authorities, and therefore requires similar measures for all environmental information held by NIGALA.

2. Purpose

NIGALA acknowledges its obligations as set out under FOI and EIR, and is committed to the principles of openness, transparency and accountability.

This policy establishes a framework which underlines the commitment. The purpose of this policy and related procedures is to ensure that NIGALA is compliant with the FOI and EIR, and sets out the procedures for dealing with requests for information in an efficient manner.

3. Supporting Legislation

This policy has been written to support staff in compliance with legal requirements and best practice guidance as set out in the NIGALA's overarching Information Governance Policy.

4. Scope

The scope of this policy is to support the control and management of information. The policy will cover all information within NIGALA and is concerned with all information systems, electronic and non-electronic information. It applies to all directorates, services and departments, all permanent and temporary staff, all agency staff, and as appropriate to contractors and third party service providers acting on behalf of NIGALA.

This includes, but is not necessarily limited to information:

- stored on computers, paper and electronic structured records systems
- transmitted across internal and public networks such as email or Intranet/Internet
- stored within databases
- printed or handwritten
- stored on removable media such as CDs, hard disks, pen drives, tapes and other similar media
- stored on fixed media such as hard drives and disk subsystems
- held on film or microfiche
- information recording and processing systems whether paper electronic video or audio records
- presented on slides, overhead projectors, using visual and audio media
- spoken during telephone calls and meetings or conveyed by any other method

This policy covers all forms of information held, which includes but is not necessarily limited to:

- Information about members of the public
- Non- employees on organisational premises
- Staff and Personal information
- Organisational, business and operational information

5. Responsibilities

5.1 The **Board** has overall responsibility to ensure compliance in all areas of information governance.

5.2 The **Chief Executive** has ultimate responsibility for the delivery of this policy.

5.3 The **Personal Data Guardian (PDG)** is a senior person responsible for protecting the confidentiality of personal information.

5.4 The **Senior Information Risk Officer (SIRO)** is an executive who has responsibility to ensure compliance with legislation through the development and monitoring of policy and codes of practice

5.5 The **Head of Corporate Services** is responsible for ensuring compliance with FOI requirements.

5.6 The **Records Management Officer** is responsible for ensuring that this policy and associated procedures is kept up to date.

5.7 **The Assistant Directors** are responsible individually and collectively for the application of the Information Governance suite of policies within their groups.

5.8 The **Records Management Officer** at NIGALA will liaise with the FOI Team at BSO in the provision of information as required.

5.9 **Managers** are responsible for ensuring that this policy and its supporting standards and guidelines are built into local processes.

5.10 **All Staff** members, whether permanent, temporary or agency are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis. Staff are expected to familiarise themselves with, and abide by, the principles set out within this policy

5.11 The **Business Services Organisation** provides support and professional advice to NIGALA on Information Governance. In doing so the Business Services Organisation is considered a Data Processor as set out under GDPR. The BSO processes Freedom of Information requests on behalf of NIGALA.

6. Handling and tracking of requests

6.1 Defining a Valid FOI Request

As defined in Section 8 of the FOI Act, to meet all the retirements of a valid FOI request, a request must:

- Be in writing
- State the name of the applicant and a valid address for correspondence
- Describe the information requested
- Be received in a legible form

The term 'in writing' covers requests submitted by letter and electronic form, including those sent via Social Media. The request does not have to make any direct reference to the Act, or be the sole or main theme of the requester's correspondence.

A request is deemed as 'received' when it is delivered to NIGALA (for example, to the inbox of a member of staff), and not the date the request is forwarded for onward processing[4]. Any requests for information under FOI must therefore be forwarded to Corporate Services immediately for onward processing by the Business Services Organisation.

6.2 Identity of the applicant and reasons for the request

The ICO has advised that, as FOI enables disclosure on grounds of public interest, responses should be applicant and motive blind. NIGALA will therefore assess all requests on the understanding that applicant identity is not a relevant consideration. Possible exceptions to this include:

---

[4] In respect of emails, however, where an automated 'out of office' message provides instructions on how to re-direct a message, the request would not be 'received' until it was re-sent to the alternative contact.

- a request is deemed to be repeated;
- if disclosure would be contrary to Data Protection principles or would be likely to endanger the health and safety of any other person;
- aggregated costs in line with Fees Regulations

6.3 Time Limits for Compliance with Requests

In providing a service to NIGALA, BSO has, and continues to develop, systems and procedures to ensure that it complies with its duties to provide a response to requests within the statutory timeframe of twenty working days from the point of a valid request being received.

If it becomes clear at any stage that the above timescales cannot be met, BSO will inform the applicant in writing and give a revised deadline for completion.

6.4 Means by which information will be conveyed

When an applicant expresses a preference for communication by particular means, NIGALA so far as is reasonably practicable, will give effect to that preference.

In determining whether it is reasonably practicable, NIGALA will consider all the circumstances, including the cost of doing so. If it is determined that it is not reasonably practicable to comply with any preference expressed by the applicant, the applicant will be notified of the reasons for its determination and will provide the information by such means as which is deemed reasonable.

6.5 Approval and Signature

An initial draft will be sent to the relevant member of NIGALA's Head of Corporate Services for approval. Following this, a final draft will be submitted to NIGALA`s Chief Executive for approval and signature or, in their absence, a separate member of NIGALA`s SMT for final signature.

Signed responses will be issued to applicants via the Corporate Services Team.

7. Refusing requests

The duty to confirm or deny does not arise if:

- an exemption under FOI is applicable;
- the request is considered vexatious and/or repeated;
- a fees notice has been issued and the fee has not been paid

7.1 Exemptions

There are 24 exemptions from the right of access. Some are designated 'absolute', meaning that the duty to provide the information does not apply. Most are designated 'qualified' exemptions and require a public interest test to be applied, to decide whether the public interest in withholding the information outweighs the public interest in disclosing it.

In determining whether disclosure would be likely to prejudice the effective conduct of public affairs (Section 36 of FOI), the designated Qualified Person will decide on the exemption's engagement. In NIGALA's case, this is the Chief Executive Officer.

Where an exemption is deemed to apply to some or all of the information requested, the applicant will be notified in writing. The relevant exemption will be cited and any information that is not exempt will be provided.

If legal opinion is deemed necessary, it will be sought by the Head of Corporate Services.

7.2 Vexatious and Repeated Requests

A request can be treated as vexatious where NIGALA can demonstrate an affirmative response to one or more of the following questions:

- Could the request fairly be seen as obsessive?
- Is the request harassing the organisation or causing distress to staff?
- Would complying impose a significant burden in terms of expense and distraction?
- Is the request designed to cause disruption or annoyance?
- Does the request lack any serious purpose or value?

Section 14(2) of FOI states that a request can be refused as repeated if:

- It is made by the same person as a previous request;
- It is identical or substantially similar to the previous request; and
- No reasonable interval has elapsed since the previous request

Should an applicant make a vexatious request or 'repeated' request for identical or substantially similar information, BSO will inform the applicant in writing that they will not fulfil the request, by indicating the reason(s) why. If the request is for information recently refused, the organisation will treat the request as a request for internal review of the original decision.

7.3 Cost

BSO on behalf of NIGALA will follow the appropriate Regulations[5] in determining cost of complying with a request. Accordingly, all requests that cost less than the 'appropriate limit' of £450 (calculated at £25 per hour) to process will be complied with free of charge.

In calculating cost, BSO may only take into account the time taken to determine whether it holds the information, and to locate, retrieve and extract it. It may not take into account the time taken to consider exemptions, to seek and obtain legal advice, to consider whether a request is vexatious, to obtain authorisation to provide the information, to calculate fees or to perform any redactions.

If the estimated cost of compliance exceeds the appropriate limit, the duty to comply with the request does not arise. However, in keeping with the duty to provide advice and assistance, NIGALA will first seek to refine the request with the applicant in order to provide relevant and useful information within the limit appropriate limit.

If NIGALA is intending to charge a fee, it must issue a fees notice to the applicant. In the event of a fees notice being issued, the twenty working day compliance period is placed 'on hold' from the date of issue until the fee is received. If no fee is received, the request will be closed three months from the date of fees notice.

No 'appropriate limit' is set by EIR. However, NIGALA reserves the right to refuse to comply with requests under Section 12(4) of EIR which are 'manifestly unreasonable' or 'too general'. As with FOI, BSO has a duty to advise the applicant on how to re-focus the request to one that would be acceptable.

8. Internal Review

Applicants may ask NIGALA to conduct an Internal Review of its handling of FOI / EIR requests.

Internal Reviews consider decisions made, rationale, public interest, timeliness and all other relevant aspects of the request.

Internal Review Panels will consist of two NIGALA members of staff with no involvement in the original handling of the request, and preferably a member of SMT

NIGALA will conduct internal reviews within 20 working days or 40 working days where a review is shown to be particularly complex.

[5] The Relevant Fees Regulation is The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

The review panel will reserve the right to interview members of staff involved in the original decision, in order to better inform their decision. A response will be signed by both members of the review panel, and issued to the applicant via Corporate Services.

Applicants who may remain unsatisfied with the outcome of an Internal Review will be advised that they may exercise their right to appeal to the Information Commissioner.

9. Transferring Requests for Information

It is NIGALA policy not to contact another authority on the applicants' behalf to transfer the request. However, in circumstances where NIGALA believe that the information requested is held by another public authority, it will:

- advise the applicant that NIGALA will not be taking the request further;
- provide contact details of that authority

10. Consultation with Third Parties

Where disclosure cannot be made without the consent of a third party and would constitute an actionable breach of confidence such that an exemption would apply, NIGALA will consult that third party with a view to seeking their consent, unless such consultation is not practicable. NIGALA may also undertake consultation where the views of the third part may assist in determining:

- whether an exemption applies, or
- where the Public Interest lies

NIGALA may consider that consultation is not appropriate where:

- the cost of consulting with the third party would be disproportionate;
- the view of the third party can have no effect on the decision as to whether to disclose;
- an exemption applies

In such cases it will consider the most reasonable course of action to take in light of the requirements of FOI. Equally, a refusal to consent to disclosure by, or lack of response from, a third party does not automatically mean information will be withheld. At all times, NIGALA will consider its duty under FOI.

11. Publication Scheme

FOI makes it a duty for NIGALA to adopt and maintain a scheme relating to the publication of its information. NIGALA has adopted the 'approved model' Publication Scheme introduced by the Information Commissioner's Office, and can be found on its website.

12. Performance and Monitoring Compliance

The effectiveness of this policy will be assessed on a number of criteria:

- compliance with legislation in respect of FOI;
- performance against agreed standards on an annual basis

13. Non-Compliance

A failure to adhere to FOI, this policy and any associated procedures may result in disciplinary action. In relation to the use of ICT Equipment including the use of the. Internet and Email, staff should be aware that they might be personally liable to prosecution if their actions are found to be in breach of the law. Serious breaches may be reported to the PSNI, ICO or other public authority for further investigation.

Appendix 5 – Information Security

Table of Contents

1 Introduction

1.1 Due to the sensitive and confidential patient and personal data captured, along with commercially sensitive information, and the reliance on information systems to process and transmit data to stakeholders, Information Security (IS) is fundamental to the operation and success of all HSCNI bodies and of paramount importance to meet the organisations' primary objectives.

1.2 This policy has been written to support staff in compliance with legal requirements and best practice guidance as set out in the NIGALA's overarching Information Governance Policy.

1.2 This policy:

- applies to all business functions and covers all information systems, networks, physical environment and relevant people who support those business functions
- sets out the policy for the protection of the confidentiality, integrity and availability of their information assets
- establishes the security responsibilities for information security
- outlines the approach to information security management
- describes the responsibilities necessary to safeguard the security of information

2 Purpose

2.1 The objectives of this policy are to:

- ensure the security of information assets
- ensure that information assets are available as and when required, in order to meet business objectives
- protect information assets from unauthorised or accidental modification or destruction or unauthorised disclosure, in order to ensure the accuracy and completeness of the information assets
- minimise risk to information

2.2 The aim of this policy is to establish and maintain the security and confidentiality of Information assets by:

- ensuring that all members of staff are aware of, understand and fully comply with the relevant legislation as described in this and other policies
- describing the principals of information security and explaining how they will be implemented
- introducing a consistent approach to information security, ensuring that all members of staff fully understand their own responsibilities
- creating and maintaining a level of awareness of the need for IS as an integral part of the day to day business
- protecting information assets
- informing the Chief Executive of each signatory body to assist with the statement of internal control made by him/her
- protecting the signatory bodies from liability or damage through the misuse of its information

3 Scope

3.1 This policy relates to the use of all organisation-owned information assets (both physical and system based), network applications, to all privately owned systems when connected directly or indirectly to the network and to all organisation-owned and/or licensed or sanctioned software/data and equipment. This includes, but is not necessarily limited to:

- stored on computers
- transmitted across internal and public networks such as email or Intranet/Internet
- stored within databases
- printed or handwritten on paper, whiteboards (etc.)
- sent by facsimile (fax), telex or other communications method
- stored on removable media such as CDs, hard disks, pen drives, tapes and other similar media
- stored on fixed media such as hard drives and disk subsystems
- held on film or microfiche
- paper and electronic structured records systems
- information recording and processing systems whether paper electronic video or audio records
- presented on slides, overhead projectors, using visual and audio media
- spoken during telephone calls and meetings or conveyed by any other method

3.3 This policy covers all forms of information held, including (but not limited to):

- information about members of the public
- staff and personal information
- organisational, business and operational information

3.4 This policy covers all information systems purchased, developed and managed by/or on behalf of the signatory bodies

3.5 This policy applies to all directorates, services and departments, all permanent and temporary staff, all agency staff, and as appropriate to contractors and third party service providers acting on behalf of the signatory bodies.

4 Responsibilities

4.1 The Chief Executive Officer (CEO) is the **Accountable Officer** and has overall responsibility for ensuring that information security is applied.

4.2 The **Personal Data Guardian (PDG)** is responsible for acting as a central point of contact on IS

4.3 The NIGALA **PDG** is responsible for:

- ensuring that the IS policy is produced and kept up to date
- producing operational standards, procedures and guidance on IS matters for approval by the Information Governance Management Committee (IGMC)
- co-ordinating IS activities, particularly those related to shared information systems or ICT infrastructures

- liaising with external organisations on IS matters, including reporting IS breaches to the ICO as appropriate and representing the organisations on cross-community committees
- reporting to the IGMG on matters relating to IS

4.4 The **Senior Information Risk Owner (SIRO)** will be responsible for managing and implementing information security policies and procedures

4.5 The responsibilities of the **Information Asset Owners (IAOs)** include:

- leading and fostering a culture that values, protects and uses information appropriately
- knowing what information is held, and what and how information is transferred
- knowing who has access to each information asset, and ensuring that access / use of each information asset is monitored and controlled
- understanding and addressing risks to IS and providing assurance to the SIRO
- ensuring any data breach incidents are appropriately reported and managed

4.6 The responsibilities for the **Head of Corporate Services** include the provision of technical and administrative support to all staff in conducting their delegated responsibilities. The **Head of Corporate Services** has day to day responsibility for ICT Security. This includes the maintenance and review of the ICT Security Policy and subordinate policies and procedures

4.7 **Managers** are responsible for:

- overseeing the implementation of IS within their area of responsibility
- agreeing, alongside ITS, the most appropriate system security policies for each information system
- the security of the assets is consistent with legal and management requirements ensuring that systems are tested and agreeing subsequent rollout plans
- advising SMT on the accreditation of systems, applications and networks
- providing a business area point of contact on IS issues
- contacting the relevant director / assistant director when
  - incidents or alerts have been reported that may affect systems, networks or applications
  - proposals have been made to connect to systems, networks or applications that are operated by external parties
- ensuring that staff are aware of their security responsibilities and have had suitable training

4.8 **All Staff**, whether permanent, temporary or agency, or agents acting for or on behalf of NIGALA(including Self Employed Guardians) are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with this policy. This includes:

- the operational security of the information systems they use
- preventing the introduction of malicious software on ICT systems
- reporting on any suspected or actual breaches in security

5 Policy Framework

5.1 **Supporting Policies, Codes of Practice, Procedures and Guidelines** have been developed to strengthen and reinforce this policy. These are available for viewing on the NIGALA website.

5.2 **Human Resources**

5.2.1 **Training**: Information security awareness training will be included in the staff induction process. An on-going awareness programme will be established in order to ensure that staff awareness is refreshed and updated as necessary.

5.1.2 **Contracts**: Security requirements will be addressed at the recruitment stage and all contracts of will contain an appropriately worded confidentiality clause. Information Security Requirements will be included in job descriptions.

5.1.3 **Contracts with external contractors** must be in operation before access is allowed to information systems, and must include clauses about information and ICT security and protection. These agreements will require staff or sub-contractors of the external organisation to comply with all appropriate security policies.

5.3 **Asset Security**

All ICT equipment and equipment for the handling of information will:

- be recorded on the corporate registers
- be physically protected from security threats and environmental hazard
- have a named custodian who will be responsible for the security of that asset

5.4 **User Access Controls**: Access to ICT equipment, systems and information will be restricted to authorised users who have a business need to access the information.

5.5 **Computer and Network Procedures**: Management of computers and networks will be controlled by standard procedures.

5.6 **Security Incidents**: All security incidents are to be reported to the ITS Security Manager or the IGC. All security incidents will be investigated to establish their cause, operational impact, and business outcome.

In the event of a suspected or actual security breach the SIRO may, after with the relevant senior staff, authorise action to remove or restrict access to systems, facilities and information or anything else deemed reasonable to secure information.

5.7 **Protection from Malicious Software**: The NIGALA will use software countermeasures and management procedures to protect itself against the threat of malicious software. Users must not install software on computing assets without approval.

5.8 **Removable Media**: Removable media must be approved for use, and encrypted and fully virus checked before being used on ICT equipment.

5.9 **Accreditation of Information Systems**: All new information systems, applications and networks must be compliant with organisational requirements and include a security policy and plan that is agreed by the PDG or, if unavailable, the relevant Director before they commence operation.

5.10 **System Change Control:** Changes to information systems, applications or networks must be reviewed and agreed with the appointed IAO and the SIRO/Data Guardian.

5.11 **Intellectual Property Rights:** The NIGALA will ensure that all information products are properly licensed and approved by ITS. Staff must not install software on computing assets.

5.12 **Business Continuity and Disaster Recovery Plans**: The NIGALA will ensure that business continuity and disaster recovery plans are produced for all critical information, applications, systems and networks.

5.13 **Reporting:** The Head of Corporate Services will keep the SIRO/Data Guardian, SMT and IGMC informed of the information security status by means of annual reports.

6 Performance and Monitoring Compliance

6.1 The effectiveness of this policy will be assessed on a number of criteria including the management (including frequency) of information security breaches, including near misses.

6.2 The NIGALA will audit information security management practices for compliance with this policy. The audit will:

- identify areas of operation that are covered by this policy
- follow a mechanism for adapting the policy to cover missing areas if these are critical to the management of information security, and use a subsidiary developmental plan if there are major changes to be made
- set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance
- highlight non-conformance
- report the audit results to SMT and IGMG

7 Non-Compliance

7.1 A failure to adhere to the policy and its associated procedures/guidelines may result in disciplinary action and /or dismissal. Any breach of policy will be investigated and disciplinary action may be taken regardless of whether organisational equipment or facilities are used for the purpose of committing the breach. In relation to the use of ICT Equipment including the use of the Internet and Email, staff should be aware that they might be personally liable to prosecution and open to claims for damages if their actions are found to be in breach of the law. Serious breaches may be reported to the PSNI, ICO or other public authority for further investigation.