DATA PROTECTION POLICY

Published: March 2010

Last Reviewed: June 2015
Next Review Due: June 2018

Contents List

Appendices

1 Purpose

1.1 The Northern Ireland Local Government Officers' Superannuation Committee (NILGOSC) holds a significant amount of personal data, mainly belonging to Scheme members, staff and Committee members. NILGOSC aims to achieve best practice standards in managing its information as well as compliance with information law. This policy sets out the standards which NILGOSC applies when managing personal data, in order to ensure:

- Compliance with legal obligations
- Adherence to best practice guidelines
- Protection of our members, staff and Committee members.

2 Scope

2.1 This policy applies to:

- NILGOSC staff and Committee members
- Scheme members and employing authorities
- Third party service providers and contractors working on behalf of NILGOSC
- Personal data in any medium that is not already in the public domain.

3 Legislative Framework

3.1 The EU Data Protection Directive (95/46/EC) is designed to protect the privacy of all personal data collected for or about EU citizens. The Data Protection Act 1998 (the DPA) came into force on 1 March 2000 and is how the UK implements the EU Directive. The DPA substantially broadened data protection legislation in the UK and established a framework of rights and duties designed to safeguard personal data. The Freedom of Information Act 2000 also amended the Data Protection Act for all "public bodies" by widening the definition of personal data.

3.2 The DPA has the following two aims:

- To protect individuals' fundamental rights and freedoms, notably privacy rights in respect of personal data processing
- To enable organisations to process personal information in the course of their legitimate business.

3.3 The effective implementation of this policy is critical to ensuring NILGOSC's compliance with the legislative requirements governing personal data and privacy, namely the DPA and the Human Rights Act (1998).

3.4 Compliance with the DPA is monitored by the Information Commissioner's Office (ICO), an independent authority which has the power to take action against individuals or organisations which do not comply with the DPA. These powers include criminal prosecution, non-criminal enforcement, including issuing undertakings and enforcement notices, and audit. The ICO also has the power to serve a monetary penalty notice on a data controller, up to the value of £500,000.

3.5 The following legislation, international standards and Government requirements are also applicable:

- Freedom of Information Act (2000)
- Environmental Information Regulations (1992) & Environmental Information (Amendment) Regulations (1998)
- ISO 15489 -1 and ISO 15489 -2 Information and Documentation - Records Management
- ISO 27001- Information technology - Security techniques - Information Security Management Systems - Requirements
- Data Handling Procedures in Government: Final Report, Cabinet Office, June 2008
- HMG Security Policy Framework, Cabinet Office, July 2014
- Privacy and Electronic Communications (EC Directive) Regulations 2003

4 Notification

4.1 Under the terms of the DPA, every organisation must notify the ICO of the data they hold and the purpose for processing, for inclusion in the Data Protection Register. This notification must be renewed on an annual basis. Failure to do so is a criminal offence.

4.2 NILGOSC's Data Protection registration number is Z5698603. The register entry notes that personal data is held by NILGOSC in its capacity as "Trustees of a Pension Scheme"[1].

5 Definitions

5.1 Some of the common definitions used in this policy and procedures are set out below:

5.2 ***Data*** can be factual information, such as names and addresses, or it can be expressions of opinion or intention and can occur in any format, e.g. Word documents, paper files, databases, spreadsheets, e-mails, microfilm, etc. Data is information which is:

- Processed on computer and/or in manual form;
- Recorded with the intention of processing on computer or manually;
- Recorded and kept electronically or manually; or
- Recorded information held by NILGOSC as a public authority, which does not fall within the above definitions.

5.3 ***Personal data*** means data which relates to a living identifiable individual. This may also include visual material, such as videos, photographs and CCTV images.

5.4 ***Sensitive personal data*** means personal data consisting of information which may include any of the following: racial or ethnic origin, political opinions, religious beliefs, membership of a trade union, physical or mental health, sexual orientation, actual or alleged criminal offence(s).

5.5 ***Processing data*** means obtaining, recording or holding the information, or carrying out any operation on the information such as organisation, retrieval, disclosure or destruction.

[1] This is a standard "Nature of work" description used by the Information Commissioner's Office for registration purposes.

5.6 ***Data controller*** means the person or organisation responsible for deciding what personal data is obtained, and how it is to be used. NILGOSC is the data controller for the personal data it holds, or which is processed under its instructions.

5.7 ***Data subject*** means an individual who is the subject of personal data. For NILGOSC, this includes Scheme members, their partners and dependants, staff and Committee members.

6 Data Protection Principles

6.1 The DPA details eight key principles which determine how personal data must be processed. In accordance with these principles, NILGOSC will ensure that:

1. Personal data is processed fairly and lawfully and, in particular, is not processed unless:

   a) at least one of the conditions in Schedule 2 is met, and
   b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data is obtained only for one or more specified and lawful purpose, and is not further processed in any manner incompatible with that purpose.

3. Personal data is adequate, relevant and not excessive in relation to the purpose for which it is processed.

4. Personal data is accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose is not kept for longer than is necessary for that purpose.

6. Personal data is processed in accordance with the rights of data subjects under the DPA.

7. Appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data is not transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The EEA consists of EU Member states, Liechtenstein, Iceland and Norway and includes Gibraltar as part of Great Britain. The Isle of Man and Channel islands are not part of the EEA.

7 Data Protection Policy Statement

7.1 NILGOSC is committed to full compliance with the DPA. This policy statement and the Data Protection Procedures set out how NILGOSC aims to implement the DPA requirements in relation to the collection, storage, use and transfer of personal data.

7.2 NILGOSC will ensure that the retention and management of personal data comply with the DPA. NILGOSC recognises that there is a need to receive, process and retain personal data but acknowledges that:

- personal data will be held for legitimate business purposes only
- it will be accessible to staff members on a need to know basis only
- it will be accessible to individuals who wish to inspect data about themselves, providing this does not breach the confidentiality of a third party
- it will not be used in a manner incompatible with the reasons for which it has been collected and is held
- at the point of collecting data, individuals will be informed of the purpose and use of that data, and consent will be acquired where appropriate.

7.3 NILGOSC will ensure that the processing of personal data and sensitive personal data complies with the conditions set out in Schedules 2 and 3 of the DPA, provided at Appendix A and Appendix B respectively.

7.4 No data will be disclosed to a third party unless the individual has given their written consent, or the third party has a statutory or legal authorisation to be supplied with the information. Fair processing notices will ensure that NILGOSC is open and transparent about the use of the personal data it holds.

7.5 NILGOSC's Retention and Disposal Schedule lists, amongst other corporate records, the personal datasets that it holds, and the retention periods put into place to ensure that those records are not retained for any longer than necessary.

7.6 In addition to this policy, the following internal policies and guidance aim to maintain the confidentiality, integrity and availability of the personal data which is held by NILGOSC:

- Data Protection Procedures
- Information Security Policy
- Information Risk Policy
- Document Management Policy
- Freedom of Information Policy and Procedures
- Secure Desk Guidance

8 Key Personal Data Risks

8.1 The effective management of personal data is not simply about ensuring compliance with the DPA, but about following best practice guidelines for information security, information risk management and openness, accountability and transparency.

8.2 Personal data is a particularly sensitive type of information held by NILGOSC, and is factored into our information risk management processes. The key potential risks which this policy is designed to address are:

- Breach of confidentiality (information being disclosed inappropriately)
- Breach of security (unauthorised access to information)
- Failure to produce fair processing notices or to gain positive consent
- Failure to establish efficient systems of managing change, leading to personal data not being up to date
- Insufficient clarity to staff and the public about the way data is used

- NILGOSC's service provider(s) failing to comply with, or to support, this data protection policy

8.3 NILGOSC assesses information risks in line with the Risk Management Policy, and information risks are recorded in the corporate risk register.

9 Roles and Responsibilities

9.1 All staff have a responsibility to manage personal data held by NILGOSC appropriately, in accordance with the Data Protection Policy and Data Protection Procedures. In addition, the roles listed below have specific information management responsibilities.

9.2 *Senior Management Team:* Overall responsibility for ensuring that NILGOSC complies with legal obligations, with this policy and with the Data Protection Procedures.

9.3 *Senior Information Risk Owner (SIRO):* This role is currently fulfilled by the Deputy Secretary, whose responsibilities include:

- Designated Data Controller for NILGOSC
- Owner of the Information Risk Assessment and the Information Risk Policy
- Provision of written advice to the Accounting Officer on the content of the annual Governance Statement in regard to information risk
- Oversight of appropriate controls to manage and mitigate personal data risks, including training for staff, managers and Committee Members
- Ensuring that NILGOSC information management policies are maintained.

9.4 *Data Protection Officer/Information Risk Manager*: This role is currently fulfilled by the Information & Compliance Manager, whose responsibilities include:

- Maintaining, reviewing and monitoring compliance with NILGOSC's information management policies
- Briefing the SIRO on data protection responsibilities
- Handling Subject Access Requests
- ICO notification, including the reporting of personal data breaches
- Advising other staff on data protection issues
- Ensuring that data protection induction and training take place
- Conducting a biennial review of information risk and the effectiveness of the information risk policy
- Approval of contracts with Data Processors.

9.5 *Information Security Officer*: This role is undertaken by the IT Systems Manager, who has the following responsibilities:

- Day to day responsibility for all aspects of information security
- Making decisions on information security matters
- Implementation and review of the Information Security Policy
- Information security incident reporting and resolution
- Provision of staff training on information security.

9.6 *Information Asset Owners (IAOs):* All teams in NILGOSC handle personal data. The IAO role is undertaken by Senior Managers responsible for each team in respect of the information assets and systems under their control. The role has the following responsibilities:

- Knowing what information is held, who has access and for what purpose

- Ensuring that good data protection practice is followed by ensuring that staff adhere to the guidance set out in this policy and the Data Protection Procedures
- Understanding, identifying and responding to risks to information assets and systems
- Identifying and keeping a record of staff and contractors with access to, or involved in handling, individual records containing personal data
- Approving arrangements for the transfer of data, e.g. on removable media
- Approving information disposal mechanisms.

9.7 *All NILGOSC staff* are responsible for:

- Following policies and procedures for managing personal data
- Advising the Data Protection Officer or SIRO when they believe that the DPA and/or this policy may have been breached
- Forwarding any Subject Access Requests to the Data Protection Officer for processing
- Ensuring that any information they provide to NILGOSC in connection with their employment is accurate and up to date.

The Data Protection Procedures provide further details on generic staff responsibilities for data protection.

9.8 These responsibilities apply equally to full-time and part-time staff, temporary and agency staff, contractors and consultants.

9.9 Breaches of this policy may result in disciplinary action.

10 Staff Awareness and Training

10.1 All staff must successfully complete an e-learning course in respect of data protection and must pass the associated test within four weeks of joining NILGOSC. Staff are also required to attend a mandatory training session on data protection and information security as part of their induction process.

10.2 All staff must undertake mandatory annual data protection refresher training.

10.3 In addition, guidance on handling personal data is provided to staff via the corporate intranet.

11 Monitoring and Review

11.1 The SIRO will oversee the operation of this policy on behalf of the Senior Management Team. This will include a review as part of the triennial information risk assessment.

11.2 The Data Protection Policy and Data Protection Procedures were published in March 2010. They will be reviewed every three years, but may be reviewed more regularly to reflect any changes to relevant legislation.

Published:	March 2010
Updated:	November 2011
Updated:	January 2013
Last Updated:	June 2015
Next Review Due:	June 2018

Appendix A

SCHEDULE 2

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1. The data subject has given his consent to the processing.

2. The processing is necessary—

a) for the performance of a contract to which the data subject is a party, or
b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary—

(a) for the administration of justice,
(aa) for the exercise of any function of either House of Parliament,
(b) for the exercise of any functions conferred on any person by or under any enactment,
(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6. (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Appendix B

SCHEDULE 3

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA

1. The data subject has given his explicit consent to the processing of the personal data.

2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
(2) The Secretary of State may by order—
(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary—
(a) in order to protect the vital interests of the data subject or another person, in a case where—
(i) consent cannot be given by or on behalf of the data subject, or
(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing—
(a) is carried out in the course of its legitimate activities by any body or association which—
(i) is not established or conducted for profit, and
(ii) exists for political, philosophical, religious or trade-union purposes,
(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing—
(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
(b) is necessary for the purpose of obtaining legal advice, or
(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. (1) The processing is necessary—
(a) for the administration of justice,
(aa)for the exercise of any function of either House of Parliament,
(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
(2) The Secretary of State may by order —
(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

7A. (1) The processing—
(a) is either—
(i) the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or
(ii) any other processing by that person or another person of sensitive personal data so disclosed; and
(b) is necessary for the purposes of preventing fraud or a particular kind of fraud.
(2) In this paragraph "an anti-fraud organisation" means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes

8. (1) The processing is necessary for medical purposes and is undertaken by—
(a) a health professional, or
(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. (1) The processing—
(a) is of sensitive personal data consisting of information as to racial or ethnic origin,
(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.
(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.