North East Scotland Pension Fund

nespf

Data Protection Policy

May 2023

Contents

Document	**Data Protection Policy**
Draft/Review Date	May 2023
Approval Date	June 2023
Author & Team	M Suttie, Governance Team
Review Date	May 2024

Purpose Statement

This policy has been prepared, on behalf of Aberdeen City Council as the administering authority for the North East Scotland Pension Fund (NESPF) (the 'Fund').

This policy details the Fund's responsibilities in terms of data protection and provides an overview of how the Fund meets data protection obligations in its working practices.

Application and Scope

The data protection obligations set out within this policy apply to all Pension Fund staff.

The General Data Protection Regulation (GDPR) replaced the EU Data Protection Directive of 1995 (95/46/EC) and supersedes the laws of individual Member States that were developed in compliance with the Directive. Its purpose is to protect the 'rights and freedoms' of natural persons (i.e. living individuals) and to ensure personal data is not processed without the individual's knowledge, and, wherever possible, it is processed with their consent. The GDPR applies to all 'data controllers' established in the European Union who process the personal data of 'data subjects'.

Following the United Kingdom's exit from the EU (or Brexit) the GDPR is retained in domestic law as the UK GDPR, but the UK has the ability to keep the framework under review. The UK GDPR sits alongside an amended version of the Data Protection Act 2018. The key principles, rights and obligations remain the same. However there are implications for the rules on transfers of personal data between the UK and European Economic Area (EEA).

Personal data is defined as information which relates to a living individual and from which that individual can be identified, either directly or indirectly. As per Article 4 of the UK GDPR:

> *'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.*

Local Government Pension Scheme (LGPS)

The Fund must identify a lawful basis on which it can process an individual's data (known as conditions for processing) and must be able to evidence to the individuals concerned how it meets those conditions and what their rights are for ensuring their data is managed appropriately.

The Fund is required to collect, hold, process and transfer personal data about individuals in order to carry out and fulfil its statutory functions and objectives i.e. to comply with the LGPS (Scotland) Regulations.

Data Controller

Aberdeen City Council as the administering authority for the Pension Fund is the 'data controller' under the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The data controller is responsible for deciding how and why personal data is managed.

Data Protection Officer

Public Authorities are required under the UK GDPR to appoint a Data Protection Officer (DPO) to assist with monitoring legal compliance, to inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessment's (DPIA's) and act as a contact point for data subjects and the Information Commissioner.

The DPO for Aberdeen City Council can be contacted at:

Chief Officer-Governance
Level 1 South, Marischal College
Broad Street, Aberdeen
AB10 1AB

Email: DataProtectionOfficer@aberdeencity.gov.uk

The Commissioner

The Information Commissioners Office (ICO) is the UK's Independent body responsible for upholding information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO is responsible for supervising compliance with the UK GDPR and dealing with complaints. Further information is available at https://ico.org.uk.

Compliance with the principles of UK GDPR

The data protection principles in Article 5 of the UK GDPR set out the main responsibilities for organisations. The Pension Fund must be able to evidence its compliance with these principles.

Principle	Funds Compliance
Personal data shall be: **a) Processed lawfully, fairly and in a transparent manner in relation to individuals**	NESPF provides benefits to approximately 72,000 plus members (active, pensioner and deferred pensioner). Members' receive new start information from their employer and a 'new start pack' from NESPF confirming membership of the Fund. The new start pack refers members to the NESPF website and the Fund's Privacy Notice which details the conditions for processing personal data, how the Fund uses the personal information and with whom it is shared.
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is not compatible with those purposes	NESPF receives member data from scheme employers on a monthly basis directly through I-Connect. It also receives information directly from its members e.g. on previous pension rights – information that the Fund requires to administer a member's pension under the LGPS (Scotland) Regulations. Some data e.g. nomination details, is collected from members which, although not immediately relevant, may be required later to allow the Fund to meet its administrative obligations.
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	A review of data held by the Fund will be carried out on a regular basis to ensure data is adequate, relevant and necessary for the purposes it was collected for. Some data e.g. nomination details, is collected from members which, although not immediately relevant, may be required later to allow the Fund to meet its administrative obligations.
	NESPF's online Member Self Service (MSS) facility allows members to log in and view their own pension account. Members can check and

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay	amend personal details which helps ensure accurate and up to date details are held at all times. NESPF receives monthly employment data from scheme employers for its active members through I-Connect. Again, this helps to ensure active member information is accurate and up to date. Annual benefit statements are delivered online for active and deferred members. Members will log into the MSS facility to view their statements and keep their personal details up to date. A Data Quality Improvement Plan is in place for the Pension Fund and includes carrying out regular tracing exercises for 'gone away' members. The Fund's Privacy Notice is available at www.nespf.org.uk.
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.	The Fund, in meeting its statutory duties under the LGPS (Scotland) Regulations has determined that it cannot permanently delete member records. However it will take necessary steps to ensure it only holds information in a manner compliant with these principles.
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.	Pension Fund staff will be required to adhere to the ACC IT Acceptable Use Policy and Corporate Information Handbook. In addition, the Fund has also produced its own written procedures around system access e.g. to the benefit administration system.

Individuals Rights under the UK GDPR

Certain rights are granted to data subjects (i.e. the members' whose data is held):

The right to be informed

This right relates to how the Fund uses an individual's information and who the information is shared with.

The Fund's privacy notice will be kept up to date and published online at www.nespf.org.uk.

The right of access

This right enables individuals to verify that the Fund is using their data appropriately and request access to copies of any information it holds.

Pension Fund members can access their individual pension account through the online NESPF Member Self Service (MSS) facility at www.nespf.org.uk. Otherwise they can contact the Fund directly to see and/or request a paper copy. Copies of the information will be provided within one month of receiving the request unless the request is complex. If this is the case the individual will be notified of any delay. Procedure notes are available to Pension Fund staff to assist with dealing with Subject Access Requests.

The right to rectification

Individuals have the right to have information amended or rectified.

Pension Fund members can check and amend their personal data through the Fund's online Member Self Service (MSS) facility available at www.nespf.org.uk or they can contact the Fund directly.

The right to erasure/right to be forgotten

This allows individuals the right to request the erasure of personal data. However it is not an absolute right and only applies in certain circumstances.

The Pension Fund in providing statutory duties under the LGPS (Scotland) regulations cannot permanently delete a member's record. However, for example, where a member transfers out or leaves with a refund of contributions, the Fund may decide to only retain the most basic record to permit it to comply with statutory and legal obligations.

The Pension Fund will keep under review the information it retains and will ensure data is erased once it no longer needs to be retained for the purposes of administering the Scheme or for archiving

purposes in the public interest. The Local Government Association (LGA) have prepared a template personal data retention policy for use across the LGPS which NESPF has adopted.

The right to restrict processing

This gives individuals the right to limit how the Fund uses their data, including who it is shared with. A request for information to be used for limited purposes will not delete the information the Fund holds.

The Pension Fund publishes its privacy notice online which outlines how the Fund uses personal data and who it shares it with. Any request for restriction of processing must be submitted to the Pension Fund for review and action.

The right to data portability

This right allows individuals to obtain copies of the information the Fund holds in a format that is easily transferred to either individuals or another organisation.

NESPF will provide the information it holds to a new pension provider in a format they can use. However the transfer of information will not take place without written consent from the member.

The right to object

In addition to the right to limit the use of data, individuals also have a right to object to the use of their data for certain actions.

The Fund may share information with third parties, for example where we outsource our print to mail documents e.g. benefit statements, P60's. Under the UK GDPR an individual can object to the Fund sharing their data with these third parties. Should a member object the Fund will take appropriate steps to comply with the request but at the same time, still ensure it provides any information or service it needs to under its statutory obligations. Further information on data sharing is available on the Fund's website and within our Privacy Notice.

Special Categories of personal data

Under Article 9 of the UK GDPR, the processing of sensitive personal data e.g. racial or ethnic origin, political opinions, data concerning health or sexual orientation, is prohibited subject to a number of exceptions. Again, the Pension Fund relies on the fact that it needs to process this type of information in order to meet its statutory obligations under the LGPS (Scotland) Regulations.

However the Fund will seek explicit member consent when dealing with ill health early retirement applications in relation to health data.

Data Relating to Children

Personal data relating to children has to be processed under the LGPS (Scotland) Regulations and therefore explicit consent is not required.

Additional Voluntary Contributions (AVCs)

Members of the Pension Fund can enter into an arrangement to pay AVCs under Regulation 17 of the LGPS (Scotland) Regulations 2018. NESPF has an agreement in place with Prudential to provide an AVC arrangement for Fund members. Lawful processing of the personal information of members is required to provide information in relation to AVC's in compliance of the Fund's statutory obligations.

Staff Training

Data protection will form an integral part of staff training and will be subject to regular review.

Subject Access Requests

The Fund will maintain a separate procedure on how to identify and respond to Subject Access Requests under the UK GDPR.

Breaches of Law

The Fund will maintain a separate Breaches of Law procedure to follow should a personal data breach occur.

Processing Activities

The Fund will monitor and review its processing activities to ensure these are, and remain, consistent with the data protection principles and individual rights (as described above).

The Fund will ensure that where there are changes in processing or new projects, a Data Privacy Impact Assessment (DPIA) is carried out to assess the data protection risk posed to individuals (Appendix I). DPIA's are mandatory under the UK GDPR for any processing likely to result in a high risk. The Fund will seek advice from the Data Protection Officer and consult as necessary.

Ad Hoc Data Sharing

In order to fulfil its administrative role, the Pension Fund will routinely share limited data with other public sector bodies or 3rd parties e.g. AVC providers, software providers, tracing bureaus. Further information is available at http://www.nespf.org.uk/TheFund/DataProtection/PrivacyNotice/share.aspx.

Occasionally the Pension Fund will also receive ad hoc data sharing requests. All such requests must be recorded using the appropriate form, a copy of which must be forwarded to the Governance Team for monitoring. See Appendix II.

It is our decision, and not the organisation requesting it, whether we choose to disclose personal data and we must be satisfied we have the correct legal grounds for doing so. If in doubt, please consult the Governance Team or the ACC Data Protection Officer before responding to any ad hoc data sharing requests.

Responsibilities

Day to day responsibility for the implementation of this policy sits with the Chief Officer-Finance and dedicated staff within the Pensions Team.

The Pensions Committee will review this policy annually, or in the event of a policy revision and taking account of any emerging issues.

Any questions or feedback on this document should be forwarded to the **Governance Team**:

NESPF
Level 1, 2MSq
Marischal Square
Broad Street
Aberdeen
AB10 1LP

Email: governance@nespf.org.uk
Web: www.nespf.org.uk

North East Scotland Pension Fund
nespf

Appendix I

Data Privacy Impact Assessment

This Data Privacy Impact Assessment must be completed wherever there is a change to an existing process or service, or a new process of information asset is introduced that is likely to involve a new use or significantly change the way in which the Pension Fund handles personal data.

Initial Screening Questions

These questions are intended to help organisations decide whether a DPIA is necessary.

Answering 'yes' to any of these questions is an indication that a DPIA is needed so the risks can be fully identified, assessed and mitigated (see attached template). You can expand on your answers as the project develops.

Will the project involve the collection of new information about individuals?	
Will the project compel individuals to provide information about themselves?	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used for?	
Does the project involve new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition?	
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	
Will the project require you to contact individuals in ways which they may find intrusive?	

Privacy Impact Assessment Template

Step 1 – Identify the need for a DPIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example, a project proposal.

Also summarise why the need for a DPIA was identified (based on your response to the initial screening questions)

Step 2 – Describe the information flows

The collection, use and deletion of personal data should be described here - what is the nature of the data, and does it include special category data? How much data will you be collecting and using? Will it be shared? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? It may be useful to refer to a flow diagram or another way of describing data flows.

Step 3– Assess necessity and proportionality measures

What is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you ensure data quality and data minimisation? What information will you give to individuals? How will you help to support their rights? How do you safeguard any international transfers?

Step 4 – Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted (internally or externally)? How will you carry out the consultation? You should link to the relevant stages of your project management process. Consultation can be used at any stage of the DPIA process.

Step 5 – Identify the privacy and related risks

Identify the key privacy risks. Larger scale DPIA's may feed into the Pension Fund's Risk Register.

Privacy issue	Likelihood of harm (Remote, Possible or Probable)	Severity of harm (Minimal, Significant or Severe)	Overall Risk (Low, Medium or High)

Step 6 – Identify measures to reduce risk

Describe the actions you can take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems)

Risk	Solution(s)	Result: Is the risk Eliminated, Reduced or Accepted?	Residual Risk (Low, Medium or High)	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step 7 – Sign off and record outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

DPO advice provided by & date:		
Summary of DPO advice:		
DPO advice accepted and overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

Step 8 – Integrate the DPIA outcome back into the project plan

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	Date for completion of actions	Responsible for action

Contact point for future privacy concerns

Lead/Project Manager	
Job Title	
Signature	
Date	

Appendix II

Personal Information Disclosure Form

Any third party request for personal data from North East Scotland Pension Fund must be recorded. This form must be used where no local arrangements are in place for recording third party personal data requests.

Section 1: Data Requester

Organisation	
Contact Name	
Address	
Contact Telephone	
Contact Email	

Section 2: Data Requested

Data being requested	
Purpose data required for	
Potentially relevant exemptions	

Section 3: Decision and Authorisation (to be completed by Authoriser)

Will information be shared as per above request (please indicate)	**YES**	**NO**
Record basis for decision here		
Name of Authoriser		
Job Title		
Description of information shared		
Method by which information was shared		
Date information was shared		

NESPF will process the personal information provided in this form in order to efficiently administer this request for information in accordance with our powers under the UK General Data Protection Regulation, and it will be retained for three years regardless of whether we decide to disclose information or not, as part of our records of compliance with the UK General Data Protection Regulation. This information will not be shared with any third parties unless we are required to do so by law. For your rights in relation to your information please see our Privacy Notice. If you would like to find out more about the way the Council processes personal data please contact the ACC Data Protection Officer.