North East Scotland Pension Fund

nespf

Breaches of Law Policy

August 2020

Contents

Document	Breaches of Law Policy
Review Date	August 2020
Approval Date	September 2020
Author & Team	M Suttie, Governance
Review Date	July 2021

Purpose Statement

This policy has been prepared on behalf of Aberdeen City Council, as the administering authority for the North East Scotland Pension Fund and the Aberdeen City Council Transport Fund ('the Fund'), to set out the arrangements for reporting breaches of the law.

In April 2015, the Pensions Regulator (tPR) published Code of Practice No. 14 *Governance and Administration of Public Sector Pension Schemes* (the 'Code'). Although not a statement of the Law itself, the Code must be taken into account by a Court or Tribunal when determining whether any pensions related legal requirements have been met.

Breaches can occur in relation to a wide variety of tasks normally associated with the administrative functions of a pension scheme such as record keeping, internal controls, calculating benefits and for funded Pension Schemes, making investment or investment-related decisions.

This policy sets out the procedure to be followed in identifying, managing and where necessary reporting breaches of the law as they apply to the management and administration of the Fund, much of which has been drawn directly from the Pensions Regulator's Code and from Aberdeen City Council guidance in respect of personal data breaches.

Application and Scope

There are certain people that are required to report breaches of the law to tPR where they have reasonable cause to believe that a legal duty which is relevant to the administration of the Pension Fund has not been, or is not being, complied with and the failure to comply is likely to be of material significance to tPR in the exercise of any of its functions.

Responsibility to report identified breaches, in the context of public service pension schemes, rests with the following (the 'Reporters'):

- Scheme Managers (i.e. the Pensions Manager and members of the Pensions Committee)
- members of the Pension Board (i.e. the NESPF Pension Board)
- any person who is otherwise involved in the administration of a public service pension scheme (i.e. all of the Officers)
- Employers (in the case of a multi-employer Fund, any participating employer who becomes aware of a breach should consider their duty to report, regardless of whether the breach relates to, or affects, members who are its employee or those of other employers)
- professional advisers including auditors, actuaries, legal advisers and fund managers
- any other person who is otherwise involved in advising the Scheme Manager in relation to the Pension Fund

The decision whether to report an identified breach requires two key considerations to be made, as not all breaches need to be reported to tPR:

1. Is there **reasonable cause** to believe there has been a breach of the law?

2. If so, is the breach likely to be of **material significance** to tPR?

Additionally, from May 2018, the General Data Protection Regulation (GDPR) introduced a mandatory duty on organisations to report certain types of personal data breaches to the relevant supervisory authority. The supervisory authority in the United Kingdom is the Information Commissioners Office (ICO). Organisations must report within 72 hours of becoming aware of the breach, where feasible.

The Pension Fund shall be satisfied that those responsible for reporting breaches are made aware of the legal requirements and tPR guidance.

Implementing adequate procedures

Those people with a responsibility to report breaches, including Scheme Managers and Pension Board members shall establish and operate appropriate and effective procedures to ensure that they are able to meet their legal obligations.

These procedures shall enable people to raise concerns and facilitate the objective consideration of those matters. It is important that procedures allow reporters to make a judgement within an appropriate timescale as to whether to report a breach (or breaches). Reliance cannot be placed on waiting for others to report.

Reporting procedures shall include the following features:

- Obtaining clarification of the law where it is not clear to those responsible for reporting
- Clarifying the facts around the suspected breach (where they are not known)
- Consideration of the material significance of the breach taking into account its cause, effect, the reaction to it, and its wider implications, including where appropriate, dialogue with the Scheme Manager or Pension Board
- A clear process for referral to the appropriate level of seniority at which decisions can be made on whether to report to tPR or the supervisory authority (i.e. escalation to the Governance Manager or Data Protection Officer)
- An established procedure for dealing with difficult cases
- A timeframe for the procedure to take place that is appropriate to the breach and allows the report to be made as soon as reasonably practicable
- A system to record breaches even if they are not reported to tPR or the supervisory authority (the principal reason for this is that the record of past breaches may be relevant in deciding whether to report future breaches, for example it may reveal a systemic issue and under the GDPR (Article 33) a record **must** be kept of all personal data breaches) and
- A process for identifying promptly any breaches that are so serious they must always be reported

The NESPF Governance Manager will be responsible for the management and execution of the Breaches Policy and associated procedures as well as record management of breaches in the Breaches Register (the Register) (see Appendix II).

All breaches will be recorded in the Register and where a materially significant breach or likely breach has or will be reported to tPR or to the supervisory authority in the case of certain personal data breaches, the NESPF Governance Manager will be responsible for further reporting to the ACC Monitoring Officer and the Pensions Committee and Board.

Judging whether to report a breach to tPR

- **Reasonable Cause**

Reporters will ensure that where a breach is suspected, they carry out checks to establish whether or not a breach has in fact occurred. Reporters shall have reasonable cause to believe that a breach has occurred; merely having a suspicion that cannot be substantiated is not enough.

For example, a member may allege that there has been a misappropriation of Pension Fund assets where the annual accounts show that the assets have fallen. However, the real reason for the apparent loss in value of assets may be due to the behaviour of the stock market over the period. This would mean that there is not reasonable cause to believe that a breach has occurred.

Where the reporter does not know the facts or events around the suspected breach, it will usually be appropriate to check with the Pension Board or Scheme Manager or with others who are in a position to confirm what has happened. However it will not be appropriate to check with the Pension Board or Scheme Manager or others in cases of theft, or suspected fraud or if other serious offences might have been committed and where discussions might alert those implicated or impede the actions of the police or a regulatory authority. Under these circumstances the reporter shall alert tPR without delay.

If the reporter is unclear about the relevant legal provision, they shall clarify their understanding of the law to the extent necessary to form a view.

In establishing whether there is reasonable cause to believe that a breach has occurred, it is not necessary for a reporter to gather all the evidence which tPR may require before taking legal action as a delay in reporting may exacerbate or increase the risk of the breach.

- **Material Significance**

In deciding whether a breach is likely to be of material significance to tPR, those with a duty to report shall consider the following:

1. **The cause of the breach**

   The breach is likely to be of 'material significance' to tPR where it was caused by:

   - Dishonesty
   - Poor governance, inadequate controls resulting in deficient administration, or slow or inappropriate decision-making practices
   - Incomplete or inaccurate advice or
   - Acting (or failing to act) in deliberate contravention of the Law

   When deciding whether a breach is of material significance, those responsible shall consider other reported and unreported breaches of which they are aware (with reference to the Breaches Register). However, historical information should be considered with care, particularly if changes have been made to address previously identified problems.

   A breach will not normally be regarded as materially significant if it has arisen from an isolated incident for example, resulting from teething problems with a new system or procedure, or

from an unusual or unpredictable combination of circumstances. However in such a situation, it is also important to consider other aspects of the breach such as the effect it has had and to be aware that persistent isolated breaches could be indicative of wider issues.

2. The effect of the breach

With tPR's role in relation to public service pension schemes and its statutory objectives in mind, evidence in relation to any of the following matters is particularly important and likely to be of material significance:

- Pension Board members not having the appropriate degree of knowledge and understanding
- Pension Board members having a conflict of interest
- Adequate internal controls not being established and operated
- The right money not being paid to the Fund at the right time
- Internal dispute resolution procedures not having been made and/or implemented
- Information about benefits and other information about Fund administration not being disclosed to members and others
- Information about the Pension Board not being published
- Public service pension schemes not being administered properly
- Appropriate records not being maintained
- Pension Board members having misappropriated Fund assets or being likely to do so
- Repeated miscalculations or incorrect payment of benefits which have a detrimental impact on members

3. The reaction to the breach

In the event of a breach, where prompt and effective action is taken to investigate and correct the breach and its causes and, where appropriate, notify any affected members, tPR will not normally consider this to be materially significant.

A breach is likely to be of concern and material significance to tPR where a breach has been identified and those involved:

- do not take prompt and effective action to remedy the breach and identify and tackle its cause in order to minimise risk of recurrence
- are not pursuing corrective action to a proper conclusion; or
- fail to notify affected members where it would have been appropriate to do so

4. The wider implications of the breach

The wider implications of a breach shall be considered when assessing which breaches are likely to be materially significant to tPR.

For example, a breach is likely to be of material significance where the fact that the breach has occurred makes it appear more likely that other breaches will emerge in the future. This may be due to the Scheme Manager or Pension Board members having a lack of appropriate knowledge and understanding to fulfil their responsibilities or where another pension fund may be affected i.e public service pension funds administered by the same organisation may be detrimentally affected where a system failure has caused the breach to occur.

When reaching a decision about whether to report, those responsible shall consider the above points together. Reporters shall consider expert or professional advice, where appropriate, when deciding whether the breach is likely to be of 'material significance' to tPR.

Judging whether to report a breach to the ICO

All organisations are under a duty to report certain types of personal data breach to the relevant supervisory authority under recital 85 of the General Data Protection Regulation.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data e.g. where data is lost, destroyed, corrupted or disclosed; accessed or transferred without authorisation or made unavailable through accidental loss, destruction or malicious encryption.

When deciding whether a personal data breach needs to be reported to the ICO, the ACC Data Protection Officer must consider whether there is a 'risk to the rights and freedoms of individuals'. When assessing the risk to rights and freedoms it is important to focus on the negative consequences to the individual e.g. physical, material or non-material damage.

If it is likely there will be a risk then the breach must be reported. However if there is deemed to be no such risk, even though a data breach has occurred, there is no reporting obligation under the GDPR.

Submitting a report

- **To the Pensions Regulator**

Breaches shall be reported as soon as reasonably practicable depending on the circumstances. In particular, the time taken to report shall reflect the seriousness of the suspected breach.

Where possible, reports should be submitted directly on tPR's website via *Exchange*.

Alternatively, reports to tPR can be submitted **in writing** and sent by post or electronically, including by email or by fax. Reporters shall wherever practicable use the standard format available on tPR's website.

The report shall be dated and include as a **minimum**:

- Full name of the Pension Fund
- Description of the breach or breaches
- Any relevant dates
- Name of the employer or Scheme Manager
- Name, position and contact details of the reporter
- Role of the reporter in relation to the Pension Fund

In addition to the above, the following information may be helpful:

- The reason the breach is thought to be of material significance to tPR
- The address of the Pension Fund
- The contact details of the Scheme Manager (if different to the Scheme address)
- The Pension Fund registry number (if available)
- Whether the concern has been reported before

If the report is urgent, it shall be marked as such and attention shall be drawn to matters considered particularly serious by the reporter. A written report can be preceded by a telephone call, if appropriate.

In cases of immediate risk to the Pension Fund for instance, where there is any indication of dishonesty, tPR does not expect reporters to seek an explanation or to assess the effectiveness of proposed remedies. The reporter shall only make such immediate checks as are necessary. The more serious the potential breach and its consequences, the more urgently these necessary checks shall be made. In cases of potential dishonesty, the reporter shall avoid, where possible, checks which might alert those implicated. In serious cases reporters shall use the quickest means possible to alert tPR of the breach.

A reporter shall ensure they receive an acknowledgement in respect of any report they send to tPR. Only when an acknowledgement of receipt is received by the reporter can they be confident that tPR has received their report.

TPR will acknowledge all reports **within five working days** of receipt. However it will not generally keep a reporter informed of the steps taken in response to a report of a breach as there are restrictions on the information it can disclose.

Further information or reports of further breaches shall however be provided by the reporter, if this may assist tPR in exercising its functions. TPR may make contact to request further information.

- **To the Supervisory Authority**

In the case of an information security incident, an initial report detailing the information security incident must be made immediately to the ACC ICT Service Desk through ServiceNow. The ACC incident manager will be responsible for deciding whether a personal data breach is reported to the ICO.

A notifiable personal data breach must be reported to the ICO without undue delay, but no later than 72 hours after the organisation becomes aware of it. An organisation must be able to provide valid reasons for any delay in reporting.

The ICO can be notified of a breach by telephone, email or post (see https://ico.org.uk/for-organisations/report-a-breach/).

They should confirm receipt in writing within 7 calendar days.

When reporting a personal data breach, the following information must be provided:

- A description of the nature of the breach, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned

- The name and contact details of the Data Protection Officer or other contact point where more information can be obtained
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Reporting of the above information can be done in phases, where all the information isn't immediately available, provided it is done without undue further delay.

Training

The Pension Fund shall provide internal training for Scheme Managers, Pension Board members and Officers. All others shall ensure they have a sufficient level of knowledge and understanding to fulfil their duties. This means having sufficient familiarity of the legal requirements and procedures and processes for reporting.

Whistleblowing and Confidentiality

The Pensions Act 2004 makes clear that the duty to report overrides any other duties a reporter may have such as confidentiality and that any such duty is not breached by making a report. TPR understands the potential impact of a report on relationships, for example, between an employee and their employer.

The duty to report does not, however, override "legal privilege". This means that communications (oral or written) between a professional legal adviser and their client, or a person representing that client, whilst obtaining legal advice, do not have to be disclosed. Where appropriate a legal adviser will be able to provide further information on this.

TPR will do its best to protect a reporter's identity (if desired) and will not disclose the information except where lawfully required to do so. It will take all reasonable steps to maintain confidentiality, but it cannot give any categorical assurances as the circumstances may mean that disclosure of the reporters identity becomes unavoidable in law i.e. the regulator is ordered by a court to disclose it.

The Employment Rights Act 1999 ('the ERA') provides protection for employees making a whistleblowing disclosure to tPR. Consequently, where individuals employed by firms or another organisation having a duty to report disagree with a decision not to report to tPR, they may have protection under the ERA if they make an individual report in good faith. TPR expects such individual reports to be rare and confined to the most serious cases.

Aberdeen City Council has its own whistleblowing policy. The person contacted about the breach, will take this into account when assessing the case.

Supporting Procedures & Documentation

This policy is supported by other key NESPF and ACC procedures and policies, including but not limited to:

- Breaches Procedure for NESPF Staff
- ACC Whistleblowing Policy
- ACC Corporate Information Handbook
- Information Security Incident Reporting Procedure
- NESPF Breaches Register

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 any policy revision and taking account of the results from any training needs analysis and 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 1BL

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

Examples of breaches Appendix I

- An employer is late in paying over employee and employer contributions, and so late that it is in breach of the statutory period for making such payments. The employer is contacted by officers from the administering authority, it immediately pays the monies that are overdue, and it improves its procedures so that in future contributions are paid over on time. In this instance there has been a breach but members have not been adversely affected and the employer has put its house in order regarding future payments. The breach is therefore not of material significance to tPR and need not be reported.

- An employer is late in paying over employee and employer contributions, and so late that it is in breach of the statutory period for making such payments. It is also late in paying AVCs to Prudential. It is contacted by officers from the administering authority, and it eventually pays the monies that are overdue, including the AVCs to Prudential. This has happened before, with there being no evidence that the employer is putting its house in order. In this instance there has been a breach that *is* relevant to tPR in part because of the employer's repeated failures, and also because those members paying AVCs will typically be adversely affected by the delay in the investing of their AVCs.

- An employer is late in submitting its statutory year-end return of pay and contributions in respect of each of its active members and as such it is in breach. Despite repeated reminders it still does not supply its year-end return. Because the administering authority does not have the year-end data it is unable to supply, by 31 August, annual benefit statements to the employer's members. In this instance there has been a breach which *is* relevant to tPR, in part because of the employer's failures, in part because of the enforced breach by the administering authority, and also because members are being denied their annual benefits statements.

- A member of the Pensions Committee, who is also on the Property Working Group, owns a property. A report is made to the Property Working Group about a possible investment by the Fund, in the same area in which the member's property is situated. The member supports the investment but does not declare an interest and is later found to have materially benefitted when the Fund's investment proceeds. In this case a material breach has arisen, not because of the conflict of interest, but rather because the conflict was not reported.

- A pension overpayment is discovered and thus the administering authority has failed to pay the right amounts to the right person at the right time. A breach has therefore occurred. The overpayment is however for a modest amount and the pensioner could not have known that (s)he was being overpaid. The overpayment is therefore waived. In this case there is no need to report the breach as it is not material.

- An encrypted USB key containing personal data is lost or stolen. This would not be reportable to the ICO provided the data was encrypted with a state of the art algorithm and the data could be restored in good time from another source.

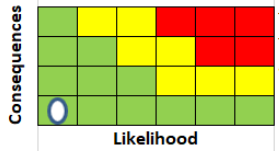
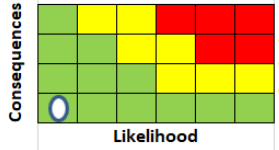
- A Pension Fund member calls the pensions office to inform it that they have been receiving documentation meant for someone else. After investigating, it is established with reasonable confidence that a personal data breach has occurred and it is likely to pose a risk to the

individual's rights and freedoms. This must be reported to the ICO. The affected individuals must also be notified if there is found to be high risk to their rights and freedoms.

NESPF 'Breaches Register' – an example

Appendix II

PENSION FUND BREACH REGISTER 2020/21

No	Date of Breach	Category	Brief Description	Potential Consequences of breach for individual(s)	Status/action to be undertaken to mitigate risk	Risk Matrix (consequences x likelihood of repeat)	Assess whether breach needs to be reported. If not, provide justification (see Breaches Policy for guidance)
1	01/04/2020	**Confidentiality Breach**	Email was sent containing scheme members (x 30) personal data (Name, NiNo, Date of Birth, Salary and Contribution details) to the wrong recipient.	Potential harm to the individuals concerned who could be identified from the personal information or the information could be used for fraudulent means	Inability to 'recall' external email. Staff to receive further training on secure email procedures. Investigate disabling auto-complete on Outlook.		Yes, the breach must be reported to the ICO as it presents a risk to the rights and freedoms of the affected individuals.
2	26/06/2020	**Availability Breach**	Personal data of member has been accidently deleted from the administration system.	Potential harm to the individual if the Pension Fund no longer has the information it needs to administer their benefits.	Ability to restore data using system back ups. Review of system processes to be carried out.		No, the incident affected only one individual, the information was only temporaily unavailable and Officers were able to restore the data in full from system back ups.

Mandatory reporting to the ICO of data breaches which are found to represent a risk to the rights and freedoms of individuals under the General Data Protection Regulation.

The Risk Matrix will be used to help identify, at a quick glance, which breaches are likely to be of material significance to tPR. It has been based on the tPR's traffic light system.

Green - not caused by dishonesty, poor governance or a deliberate contravention of the law. The effect of the breach is not significant, it is infrequent/one off or if needed, a plan is in place to rectify the situation. In such cases the breach may not be reported to tPR.

Yellow - does not fall easily into either green or red and requires further investigation in order to determine what action to take. Consideration of other recorded breaches may also be relevant in determining the most appropriate course of action. It may be necessary to informally alert tPR to a potential breach.

Red - caused by dishonesty, poor governance or a deliberate contravention of the law. The breach will have a significant impact, even where a plan is in place to rectify the situation. The Pension Fund **must** report these breaches to tPR.