A Procedure for Reporting Breaches of the Law to the Pensions Regulator

Oxfordshire Pension Fund

Reviewed June 2023

Introduction

1 In April 2015 the Pensions Regulator (the Regulator) published its Code of Practice no 14 (the Code) *Governance and administration of public service pension schemes*. This is not a statement of law of itself, but nonetheless it carries great weight. In some respects it is like the Highway Code, in that some of its contents refer to statutory items, whilst others are advisory. The Courts may however also rely on the latter. In the same way, if determining whether any pensions related legal requirements have been met, a court or tribunal must take into account the Code. This code will shortly be sub-sumed into a new General Code of Practice.

2 Subject to the legislative and regulatory requirements of the Code of Practice, the Pensions Act 2004 and the UK General Data Protection Regulation (UK GDPR), there is a statutory duty to report material breaches of the law to the Regulator or the Information Commissioner (ICO). To assist, the Code states that a procedure should be established to ensure that those with a responsibility to make reports are able to meet their legal obligations. This document is that procedure, which relates to all of the Fund's areas of operation.

3 Much of the text herein is drawn from the Code itself. Where it has been, the Regulator's copyright applies.

4 If you have any questions about this procedure and:

- You are a member of the Pension Fund Committee, Local Pension Board or you are an external adviser, please contact the Head of Pensions by emailing pension.services@oxfordshire.gov.uk;
- You are an actuary, auditor or other external agent; please contact the Head of Pensions
- You represent an employer; please contact the Pensions Services Manager by emailing pension.employers@oxfordshire.gov.uk;
- You are an officer of the Fund, and you work in Administration, please contact Pension Services Manager or Head of Pensions

Legal requirements

5 Stakeholders are required to report breaches of the law to the Regulator where they have reasonable cause to believe that:

- A legal duty which is relevant to the administration of the scheme has not been, or is not being, complied with;
- The failure to comply is likely to be of material significance to the Regulator in the exercise of any of its functions.

6 Stakeholders who are subject to the reporting requirement ('reporters') for public service pension schemes are:

- Scheme managers (meaning, in the case of the OPF the Pension Fund Committee)

- Members of the pension board - any person who is otherwise involved in the administration of the Fund (all of the Fund's officers);
- Employers, and any participating employer who becomes aware of a breach should consider their statutory duty to report, regardless of whether the breach relates to, or affects, members who are its employees or those of other employers;
- Professional advisers including auditors, actuaries, legal advisers and fund managers; and
- Any person who is otherwise involved in advising the managers of the scheme in relation to the scheme (and thus the Fund's External advisers).

Reasonable cause

7 Having 'reasonable cause' to believe that a breach has occurred means more than merely having a suspicion that cannot be substantiated.

8 Reporters should ensure that where a breach is suspected, they carry out checks to establish whether or not a breach has in fact occurred. For example, a member of a funded pension scheme may allege that there has been a misappropriation of scheme assets where they have seen in the annual accounts that the scheme's assets have fallen. However, the real reason for the apparent loss in value of scheme 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.

9 Where the reporter does not know the facts or events around the suspected breach, it will usually be appropriate to consult the Head of Pensions or Pension Services Manager, regarding what has happened. It would not be appropriate to check in cases of theft, suspected fraud or other serious offences where discussions might alert those implicated or impede the actions of the police or a regulatory authority. Under these circumstances the reporter should alert the Regulator without delay.

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

11 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 the Regulator may require before taking legal action. A delay in reporting may exacerbate or increase the risk of the breach.

Material significance

12 In deciding whether a breach is likely to be of material significance to the Regulator, it would be advisable for the reporter to consider the:

- Cause of the breach;
- Effect of the breach;

- Reaction to the breach; and
- The wider implications of the breach.

13 When deciding whether to report, those responsible should consider these points together. Reporters should take into account expert or professional advice, where appropriate, when deciding whether the breach is likely to be of material significance to the Regulator.

14 The breach is likely to be of material significance to the Regulator where it was caused by:

- Dishonesty;
- Poor governance or administration;
- Slow or inappropriate decision making practices;
- Incomplete or inaccurate advice; or
- Acting (or failing to act) in deliberate contravention of the law.

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

16 A breach will not normally be 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. But 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 scheme issues.

Effect of the breach

17 Reporters need to consider the effects of any breach, but with the Regulator's role in relation to public service pension schemes and its statutory objectives in mind, the following matters in particular should be considered likely to be of material significance to the Regulator:

- Local Board and Pension Fund Committee members not having the appropriate degree of knowledge and understanding, which may result in the Board not fulfilling its role, the Fund not being properly governed and administered and/or the Pension Fund Committee breaching other legal requirements;
- Local Board and Pension Fund Committee members having a conflict of interest, which may result in them, being prejudiced in the way that they carry out their role, ineffective governance and administration of the scheme and/or the Pension Fund Management Panel breaching legal requirements;

- Adequate internal controls not being established and operated, which may lead to the Fund not being run in accordance with the Scheme's Regulations and other legal requirements, risks not being properly identified and managed and/or the right money not being paid to or by the Fund at the right time;
- Accurate information about benefits and Scheme administration not being provided to Scheme members and others, which may result in members not being able to effectively plan or make decisions about their retirement;
- Appropriate records not being maintained, which may result in member benefits being calculated incorrectly and/or not being paid to the right person at the right time;
- Anyone involved with the administration or management of the Fund misappropriating any of its assets, or being likely to do so, which may result in assets not being safeguarded; and
- Any other breach which may result in the Fund being poorly governed managed or administered.

18 Reporters need to take care to consider the effects of the breach, including any other breaches occurring as a result of the initial breach and the effects of those resulting breaches.

Reaction to the breach

19 Where prompt and effective action is taken to investigate and correct the breach and its causes and, where appropriate, notify any affected members, the Regulator will not normally consider this to be materially significant.

20 A breach is likely to be of concern and material significance to the Regulator 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;
- Fail to notify affected scheme members where it would have been appropriate to do so.

Wider implications of the breach

21 Reporters should consider the wider implications of a breach when they assess which breaches are likely to be materially significant to the Regulator. 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 other pension schemes may be affected. For instance, public service pension schemes administered by the same organisation may be detrimentally affected where a system failure has caused the breach to occur.

Types of Breaches

Data Breaches;

22. Where a breach of security leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental or deliberate causes. It also means that a breach is more than just about losing personal data.

23. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

TPR Code of Practice Breaches:

24. These can occur for a wide variety of tasks normally associated with the administrative function of the scheme including but not limited to: -

25. **Scheme Record keeping** - Failure of employers to provide timely and accurate data for the scheme manager to fulfil their legal obligations such as when an employee joins or leaves the scheme, changes their circumstances or transfers employment between scheme employers;

26. **Maintaining contributions** - Contribution breaches occur when an employer fails to make a timely payment or consistently pays an incorrect amount. The fund are currently developing and implementing an 'Employer Contribution Escalation Policy. The policy will clearly outline the employer responsibility for payment and the fund steps for escalation which would ultimately lead to a contribution breach;

27. **Provision of information to members** - Failure to disclose information about benefits and scheme administration to relevant parties including provision of annual benefit statements to scheme members or other information as outlined under the Disclosure of Information Regulations 2013.

Examples of Code of Practice breaches
Example 1

28. 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 contacted by officers from the administering authority, it immediately pays the moneys 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 material to the Regulator and need not be reported.

Example 2

29. 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 the Prudential. It is contacted by officers from the administering authority, and it eventually pays the moneys that are overdue, including AVCs to the 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 the Regulator, 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.

Example 3

30. 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 the Regulator, 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.

Example 4

31. A member of the Pension Fund 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.

Example 5

32. 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.

Example of a Data Breach

33. Common examples of data breaches would be when the pensions administration inadvertently send information containing personal member

data, such as pension estimates, annual statements or other information to a wrong address or email. If the breach is for only one member, then that would not be a material breach. However, if the data breach involved many members, then the breach would be material.

Internal Procedure

34. Steps to follow once a breach has been identified:

    a. Record/Report breach on the internal breaches log (Excel) and on SASHA (https://sasha.oxfordshire.gov.uk/support/home). The internal breaches log can be found in the following location:

    b. Report breach to the Governance & Communications Team. At this point a determination and assessment of whether the breach is material is made in consultation with the Head of Fund. (See Paragraph 35 for how a material breach is reported to the Regulator). At this point, at the discretion of the Head of Fund, the Chair of the Pension Fund Committee may be informed and consulted;

    c. Quarterly Reporting of breaches to the Pension Fund Committee and the Local Pension Board. Each quarter Committee and Board will receive a report providing the following information on breaches:

        - Number of breaches;
        - Types of breaches (Data or Code of Practice);
        - Action taken.

Reporting a Code of Practice Breach to the Regulator

35. Before you submit a report you should obtain clarification of the law around the suspected breach. If:
    - You are a member of the Pension Fund Management Panel, Advisory Panel, Local Board or you are an external adviser, please contact the Head of Pensions
    - You are an actuary, auditor or other external agent; please contact the Head of Pensions
    - You represent an employer; please contact the Pensions Services Manager;
    - You are an officer of the Fund and you work in Administration, please contact your Pension Services Manager or Head of Pensions.

36. The person you contact will consider in the round whether the Regulator would regard the breach as being material. They will also clarify any facts, if required. If the case is a difficult one they will seek advice, as required.

37. Some matters could be urgent, if for example a fraud is imminent, whilst others will be less so. Non-urgent but material breaches should be reported to the

Regulator within 30 working days of them being confirmed, and in the same time breaches that are not material should be recorded.

38. Some breaches could be so serious that they must always be reported, for example a theft of funds by anyone involved with the administration or management of the Fund. It is difficult to be definitive about what constitutes a breach that must always be reported, but one test is: might it reasonably lead to a criminal prosecution or a serious loss in public confidence?

39. Any report that is made (which must be in writing and made as soon as reasonably practicable) should be dated and include as a minimum:

- Full name of the Fund;
- Description of the breach or breaches;
- Any relevant dates;
- Name of the employer or scheme manager (where known);
- Name, position and contact details of the reporter; and
- Role of the reporter in relation to the Fund.

40. Additional information that would help the Regulator includes:

- The reason the breach is thought to be of material significance to the Regulator;
- The address of the Fund;
- The pension scheme's registry number (if available); and
- Whether the concern has been reported before.

41. Reporters should mark urgent reports as such and draw attention to matters they consider particularly serious. They can precede a written report with a telephone call, if appropriate.

42. Reporters should ensure they receive an acknowledgement for any report they send to the Regulator. Only when they receive an acknowledgement can the reporter be confident that the Regulator has received their report.

43. The Regulator 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.

44. The reporter should provide further information or reports of further breaches if this may help the Regulator to exercise its functions. The Regulator may make contact to request further information.

45. Breaches should be reported as soon as reasonably practicable, which will depend on the circumstances. In particular, the time taken should reflect the seriousness of the suspected breach.

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

Reporting a Data Breach to the Information Commission (ICO)

47. You do not need to report every breach to the Information Commissioner and should consider the likelihood and severity of the risk to people's rights and freedoms, following the breach. If a risk is likely, you must notify the Information Commissioner; if a risk is unlikely, you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, and document it.

48. A personal data breach should be reported to the Information Commissioner without undue delay (if it meets the threshold for reporting) and within 72 hours. Reports can be made by calling the Information Commissioner helpline on 0303 123 1113 or by completing the online form on the ICO website.

Whistleblowing protection and confidentiality

49. The Pensions Act 2004 makes clear that the statutory 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. The Regulator understands the potential impact of a report on relationships, for example, between an employee and their employer.

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

51. The Regulator 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 reporter's identity becomes unavoidable in law. This includes circumstances where the regulator is ordered by a court to disclose it.

52. The Employment Rights Act 1996 (ERA) provides protection for employees making a whistleblowing disclosure to the regulator. Consequently, where individuals employed by firms or another organisation having a statutory duty to report disagree with a decision not to report to the regulator, they may have

protection under the ERA if they make an individual report in good faith. The Regulator expects such individual reports to be rare and confined to the most serious cases.

Oxfordshire County Council whistleblowing procedure

53. The Council has its own whistleblowing procedure. The person contacted about the potential breach, eg, the Solicitor to the Fund, will take this into account when assessing the case.