

## **Rhondda Cynon Taf Pension Fund (updated March 2025)**

### **Reporting Breaches Policy**

#### **Introduction**

1. The Public Services Pension Act 2013 introduced the framework for the governance and administration of public service pension schemes and provides an extended regulatory oversight by the Pensions Regulator. The Pensions Regulator General Code came into force in March 2024 replacing former separate codes.
2. The Code is not a statement of law but sets out the expectations of how governing bodies should comply with their legal duties. The Code explains that, where a breach of the law which affects the scheme may have occurred, consideration should be made as to whether this should be reported to the Pensions Regulator.

#### **Responsibility to Report**

3. Certain people are required to report breaches of the law. The requirement to report applies to:
  - the Rhondda Cynon Taf Pension Fund Committee
  - the Rhondda Cynon Taf Pension Fund Investment and Administration Advisory Panel
  - the Rhondda Cynon Taf Pension Fund Local Pension Board
  - any person who is involved in the administration of the pension fund
  - participating employers of the Rhondda Cynon Taf Pension Fund
  - all advisers, including auditors, actuaries, Fund managers, legal advisers, custodians
  - any person who is otherwise involved in advising the managers of the scheme in relation to the scheme.

#### **Decision to Report**

4. Breaches of the law which affect pension schemes should be considered for reporting to the Pensions Regulator. Not every breach needs to be reported.
5. The decision to report is based on there being reasonable cause to believe that-
  - i) A legal duty which is relevant to the administration of a scheme, has not been, or is not being, complied with; and,
  - ii) the failure to comply is likely to be of material significance to The Pensions Regulator in exercising any of their functions.

Administration is broader than day-to-day administration tasks, it includes investment policy, investment management, the custody of invested assets and scheme funding. The Pensions Regulator's interpretation of

‘administration’ covers anything that could affect members benefits, or members and others ability to access the information they are entitled to.

6. Reasonable Cause means having more than a suspicion that cannot be substantiated.
7. If a breach is suspected then checks should be carried out to determine whether or not a breach has actually taken place. However, it would not be appropriate to check in cases of theft, or if the reporter is concerned that a fraud or other serious offence might have been committed and discussion with those persons might alert those implicated or impede the actions of the police or a regulatory authority.
8. If the reporter is unclear about the relevant legal provision, they should clarify their understanding of the law to the extent to form a view.
9. 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 Pensions Regulator would require before taking legal action as any delay may exacerbate or increase the risk of the breach.

## **Material Significance**

10. The legal requirement is that breaches that are likely to be of material significance to the Pensions Regulator in carrying out its functions must be reported. Whether or not the breach is of material significance depends on:
  - the cause of the breach;
  - the effect of the breach;
  - the reaction to the breach; and
  - the wider implications of the breach.

When reaching a decision whether to report, the reporter should consider these points together.

11. The breach is likely to be of material significance to the Pensions Regulator if the breach was caused by:
  - Dishonesty, negligence, or reckless behaviour;
  - poor governance or ineffective controls resulting in deficient administration;
  - slow or inappropriate decision making practices;
  - incomplete or inaccurate advice; or
  - a deliberate act or failure to act.
12. When deciding whether a breach is of material significance, those responsible should consider other reported and unreported breaches of which they are aware. Reporters should use historical information with care, particularly if changes have been made to address previously identified problems.
13. 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.

### **Effect of the breach**

14. 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.
15. The Pensions Regulator considers a breach to be materially significant where the effects include any of the following
  - A significant proportion of members, or a significant proportion of a particular category of members are affected. The breach has a significant effect on the benefits being paid, to be paid, or being notified to members.
  - The breach, or series of unrelated breaches, have a pattern of recurrence in relation to participating employers, certain members, or groups of members.
  - Governing bodies that do not have the appropriate degree of knowledge and understanding, preventing them from fulfilling their roles and resulting in the scheme not being properly governed and administered and/or breaching other legal requirements.
  - Unmanaged conflicts of interest within the governing body, making prejudiced in the way it carries out the role, ineffective governance and scheme administration, and/or breaches of legal requirement.
  - Systems of governance (where applicable) and/or internal controls are not established or operated. This leads to schemes not being run in line with their governing documents and other legal requirements.
  - Risks are not properly identified and managed and/or the right money is not being paid to or by the scheme at the right time.
  - Accurate information about benefits and scheme administration is not being provided to scheme members and others meaning members are unable to effectively plan or make decisions about their retirement.
  - Records are not being maintained. This results in member benefits being calculated incorrectly and/or not being paid to the right person at the right time.
  - Governing bodies or anyone associated with the scheme misappropriate scheme assets or are likely to do so.

### **Reaction to the breach**

16. 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.
17. A breach is likely to be of concern and material significance to the Regulator if the breach has been identified that it:
  - does not receive prompt and effective action to remedy the breach and identify and tackle its cause to minimise risk of recurrence

- is not being given the right priority by the governing body or relevant service providers
- has not been communicated to affected scheme members where it would have been appropriate to do so
- forms part of a series of breaches indicating poor governance
- it was caused by dishonesty, even when action has been taken to resolve the matter quickly and effectively

### **Wider implications of the breach**

18. Wider implications should be considered when assessing whether the breach is likely to be materially significant to the Regulator. For example, a breach is likely to be of material significance where:
- a. the fact that the breach has occurred makes it appear more likely that other breaches will emerge in the future (the reason could be that the governing body lacks the appropriate knowledge and understanding to fulfil their responsibilities)
  - b. other schemes may be affected, for example schemes administered by the same organisation where a system failure has caused the breach
19. Those reporting a breach should consider general risk factors, such as the level of funding (in a defined benefit scheme) or how well-run the scheme appears to be. Some breaches that occur in a poorly funded and/or poorly administered scheme will be more significant to the Regulator than if they occurred in a well-funded, well-administered scheme.

### **The Traffic Light Framework**

20. When determining whether or not to report the breach the Pensions Regulator's traffic light framework should be used.
21. **Red** breach situations are always of material significance to the Pensions Regulator and should be reported. A breach is in this category if one or more of the following apply
- it was caused by dishonesty, poor scheme governance, poor advice or by deliberate contravention of the law;
  - its effect is significant;
  - inadequate steps are being taken to put matters right; or
  - it has wider implications
22. **Amber** breach situations are less clear cut; a reporter must take into account the context of the breach in order to decide whether it is of material significance and should be reported.
23. **Green** breach situations are not of material significance and do not have to be reported (but should be recorded). A breach is in this category if one or more of the following apply
- it was not caused by dishonesty, poor scheme governance, poor advice or by a deliberate contravention of the law;
  - its effect is not significant;
  - proper steps are being taken to put matters rights; and

- it does not have wider implications.

24. A decision Tree outlining the breach consideration process together with some examples obtained from 'The Pensions Regulator' is included as Appendix 1 to this policy.

### **Deciding whether a breach should be reported to the Regulator**

25. After obtaining clarification of the law, if required, and the facts around the breach the reporter should refer the potential breach to the Pensions Service Manager and Service Director, Pensions, Procurement and Transactional Services who will undertake their own investigations and, using the traffic light framework, determine whether they categorise it to be red, amber or green.
26. Any necessary courses of action to deal with the potential breach should be put in place as soon as they are identified.
27. The Service Director, Pensions, Procurement and Transactional Services will refer the case immediately to the Deputy Chief Executive and Group Director of Finance, Digital and Frontline Services (Section 151 Officer) for reporting decision.
28. If a judgement has been reached that there is reasonable cause to believe that a breach has occurred, and that it is of material significance to the Pensions Regulator, it must be reported as soon as reasonably practicable. What is reasonably practicable depends on the circumstances; in particular, the time taken should reflect the seriousness of the suspected breach.
29. To satisfy good governance and transparency, all potential and actual breaches will be formally reported (quarterly) into the Fund's Investment and Administration Advisory Panel and the Fund's Pension Board for review.

### **Making a report**

30. Reports should be made using The Pensions Regulator's on-line web from, email or post. However, if the breach is considered to have an immediate and damaging effect for scheme members, they should notify The Pensions Regulator by telephone before submitting a written report. Exchange (the Pensions Regulator's online service) should also be used by those who have access.

The report should be dated and should include as a minimum:

- name of the 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; and
- role of the reporter in relation to the scheme.

31. Additional information that would help the Regulator includes:

- the reason the breach is thought to be of material significance to the Pensions Regulator;
- the address of the Fund;
- the pension scheme's registry number; and
- whether the concern has been reported before.

32. Reports should be made as soon as reasonably practicable. In most cases this should be within 10 working days however reporters may use their judgement and apply "reasonably practicable" to their own circumstances. If it is decided that a longer reporting time is required the reasons and evidence should be recorded.
33. 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.
34. 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.
35. 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.
36. 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.
37. Cyber related incidents - trustees are also legally required to [report breaches of pensions law](#) where these are likely to be of material significance. This includes where these arise from a cyber incident, for example if it leaves you unable to process core transactions promptly and accurately, such as benefit payments. Note, this reporting does not replace existing legal requirements, such as to [report a personal data breach to the ICO](#).
38. Significant cyber incidents should be shared with the Pensions Regulator as soon as reasonably practicable. Where a significant cyber incident is likely to result in:
  - a significant loss of member data
  - major disruption to member services
  - a negative impact on a number of other pension schemes or pension service providers

## Reporting Payment Failures

39. Where it is decided that the non-payment or late payment of contributions is likely to be of material significance to The Pensions Regulator a report should be made within 14 days of there being reasonable cause to believe that a material payment failure exists.
40. The Scheme Manager has a duty to report late payment
41. Payment failures that are likely to be of material significance include:
- a. where there is reasonable cause to believe that the Fund employer is neither willing nor able to pay contributions
  - b. where there is a payment failure involving possible dishonesty or a misuse of assets or contributions
  - c. where the information available indicates that the employer is knowingly concerned with fraudulently evading their obligation to pay employee contributions
  - d. where it becomes apparent that the employer does not have adequate procedures or systems in place to ensure the correct and timely payment of contributions due and the employer does not appear to be taking adequate steps to remedy the situation
  - e. any event where contributions have been outstanding for 90 days from the due date
42. Payment failures which are not likely to be of material significance include:
- f. where a payment arrangement is being met by an employer for the recovery of outstanding contributions
  - g. where a claim has been submitted to the Redundancy Payments Office National Insurance Fund
  - h. where there are infrequent one-off payment failures
  - i. where contributions are paid late but in full and within 90 days of the due date

## Recording Breaches

43. A log of all suspected breaches, whether or not they are reported to the Pensions Regulator, will be maintained. Should similar breaches continue (for example, late payment by the same Employer), this may contribute to the materiality consideration for 'Breach' reporting purposes or indicate that insufficient action has been taken to mitigate such re-occurrences.

## Whistleblowing protection and confidentiality

44. 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

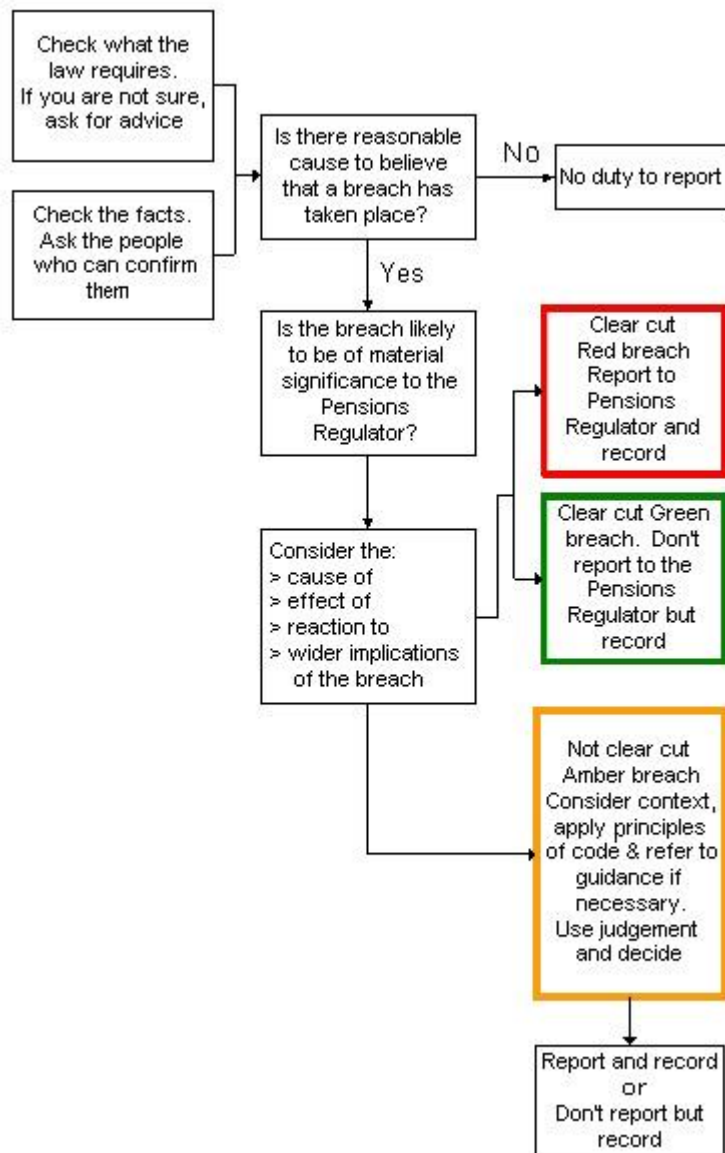
potential impact of a report on relationships, for example, between an employee and their employer.

45. The 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.
46. The Regulator will take all reasonable steps to protect a reporter's identity and maintain confidentiality, when a report is made in confidence, information will not be disclosed except where the Regulator is lawfully allowed to do so.
47. 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.
48. In all cases, reporters should act conscientiously and honestly, and to take account of expert or professional advice where appropriate.



## Appendix 1

### Decision-tree: deciding whether to report



### Example Breach of the Law and the traffic light framework - Knowledge and understanding required by pension board members

Example scenario: The scheme manager has breached a legal requirement because pension board members failed to help secure compliance with scheme rules and pensions law

	Potential Investigation Outcomes			
	Cause	Effect	Reaction	Wider Implications
	Pension Board members have failed to take steps to acquire and retain the appropriate degree of knowledge and understanding about the schemes administration policies	A Pension Board member does not have knowledge and understanding of the schemes administration policy about conflicts of interest. The pension board member fails to disclose a potential conflict, which results in the members acting improperly.	Pension Board members do not accept responsibility for their failure to have the appropriate knowledge and understanding or demonstrate negative/non-compliant entrenched behaviours.  The scheme manager does not take appropriate action to address the failing in relation to conflicts	It is highly likely that the scheme will be in breach of other legal requirements. The pension board do not have an appropriate level of knowledge and understanding and in turn are in breach of their legal requirement. Therefore, they are not fulfilling their role to assist the scheme manager and the scheme is not being properly governed.
	Pension Board members have gaps in their knowledge and understanding about some areas of the scheme's administration policies and have not assisted the scheme manager in securing compliance with internal dispute resolution requirements	Some members who have raised issues have not had their complaints treated in accordance with the scheme's internal dispute resolution procedure (IDRP) and the law	The scheme manager has failed to adhere precisely to the detail of the legislation where the breach is unlikely to result in an error or misunderstanding or affect member benefits	It is possible that the scheme will be in breach of other legal requirements. It is possible that the pension board will not be properly fulfilling their role in assisting the scheme manager
	Pension Board members have isolated gaps in their knowledge and understanding	The scheme manager has failed to adhere precisely to the detail of the legislation where the breach is unlikely to result in an error or misunderstanding or affect member benefits	Pension Board members take action to review and improve their knowledge and understanding to enable them to properly exercise their functions and they are making quick progress to address gaps in their knowledge and understanding. They assist the scheme manager to take prompt and effective action to remedy the breach	It is unlikely that the scheme will be in breach of other legal requirements. It is unlikely that the pension board is not fulfilling their role in assisting the scheme manager

### Example Breach of the Law and the traffic light framework - Scheme Record-Keeping

Example scenario: An evaluation of member data has identified incomplete and inaccurate records

	<b>Potential Investigation Outcomes</b>			
	<b>Cause</b>	<b>Effect</b>	<b>Reaction</b>	<b>Wider Implications</b>
	Inadequate internal processes that fail to help employers provide timely and accurate data, indicating a systemic problem	All members affected (benefits incorrect/not paid in accordance with the scheme rules, incorrect transactions processed and poor quality information provided in benefit statements)	Action has not been taken to identify and tackle the cause of the breach to minimise the risk of recurrence nor to notify members	It is highly likely that there are wider scheme issues caused by inadequate processes and that the scheme will be in breach of other legal requirements
	A failure by some – but not all – participating employers to act in accordance with scheme procedures, indicating variable standards of implementing those procedures	A small number of members affected	Action has been taken to identify the cause of the breach, but progress to tackle it is slow and there is a risk of recurrence	It is possible that there are wider scheme issues and that the scheme may be in breach of other legal requirements
	A failure by one participating employer to act in accordance with scheme procedures, indicating an isolated incident	No members affected at present	Action has been taken to identify and tackle the cause of the breach and minimise the risk of recurrence	It is unlikely that there are wider scheme issues or that the scheme manager will be in breach of other legal requirements

### Example Breach of the Law and the traffic light framework - Providing Information to members

Example scenario: An active member of a defined benefit (DB) public service scheme has reported that their annual benefit statement, which was required to be issued within 17 months of the scheme regulations coming into force, has not been issued. It is now two months overdue. As a consequence, the member has been unable to check:

- personal data is complete and accurate
- correct contributions have been credited
- what their pension may be at retirement

	Potential Investigation Outcomes			
	Cause	Effect	Reaction	Wider Implications
	Inadequate internal processes for issuing annual benefit statements, indicating a systemic problem	All members may have been affected	Action has not been taken to correct the breach and / or identify and tackle its cause to minimise the risk of recurrence and identify other members who may have been affected	It is highly likely that the scheme will be in breach of other legal requirements
	An administrative oversight, indicating variable implementation of internal Processes	A small number of members may have been affected	Action has been taken to correct the breach, but not to identify its cause and identify other members who may have been affected	It is possible that the scheme will be in breach of other legal requirements
	An isolated incident caused by a one off system error	Only one member appears to have been affected	Action has been taken to correct the breach, identify and tackle its cause to minimise the risk of recurrence and contact the affected member	It is unlikely that the scheme will be in breach of other legal requirements

### Example Breach of the Law and the traffic light framework - Internal Controls

Example scenario: A Defined Benefit (DB) public service scheme has outsourced all aspects of scheme administration to a third party, including receiving contributions from employers and making payments to the scheme. Some contributions due to the scheme on behalf of employers and members are outstanding.

	Potential Investigation Outcomes			
	Cause	Effect	Reaction	Wider Implications
	The administrator is failing to monitor that contributions are paid to them in time for them to make the payment to the scheme in accordance within the legislative timeframes and is therefore not taking action	The scheme is not receiving the employer contributions on or before the due date nor employee contributions within the prescribed period	The administrator has not taken steps to establish and operate adequate and effective internal controls and the scheme manager does not accept responsibility for ensuring that the failure is addressed	It is highly likely that the administrator is not following agreed service level standards and scheme procedures in other areas. The scheme manager is likely to be in breach of other legal requirements such as the requirement to have adequate internal controls
	The administrator has established internal controls to identify late payments of contributions but these are not being operated effectively by all staff at the administrator	The scheme is receiving some but not all of the employer contributions on or before the due date and employee contributions within the prescribed period	The scheme manager has accepted responsibility for ensuring that the failure is addressed, but the progress of the administrator in training their staff is slow	It is possible that the administrator is not following some of the agreed service level standards and scheme procedures in other areas. It is possible that the scheme manager is in breach of other legal requirements
	Legitimate late payments have been agreed by the scheme with a particular employer due to exceptional circumstances	The employer is paying the administrator the outstanding payments within the agreed timescale	The scheme has discussed the issue with the employer and is satisfied that the employer is taking appropriate action to ensure future payments are paid on time	It is unlikely that the employer is failing to adhere to other scheme processes which would cause the scheme manager to be in breach of legal requirements

We are asking schemes, their advisers and providers to report significant cyber incidents to us on a voluntary basis, in an open and co-operative way, as soon as reasonably practicable. You do not need to conduct the full incident investigation before reporting to us.

A significant cyber incident is likely to result in:

- a significant loss of member data
- major disruption to member services
- a negative impact on a number of other pension schemes or pension service providers

Report cyber incidents to us at: [report@tpr.gov.uk](mailto:report@tpr.gov.uk). Urgent reports should be marked as such and highlight anything particularly serious. If appropriate, you can call us after sending the report. Your advisers and service providers can also report to us for incidents at their end.

Reporting to us does not replace your existing legal requirements, such as to [report a personal data breach to the ICO](#) without undue delay (if it meets the threshold for reporting) and within 72 hours.

- Trustees are also legally required to [report breaches of pensions law](#) where these are likely to be of material significance to us. This includes where these arise from a cyber incident, for example if it leaves you unable to process core transactions promptly and accurately, such as benefit payments.
- Reporting to us does not replace trustees existing legal requirements, such as to [report a personal data breach to the ICO](#) without undue delay (if it meets the threshold for reporting) and within 72 hours.