



Remedy Breaches

10 April 2025

Clair Alcock
NPCC Head of Police Pensions



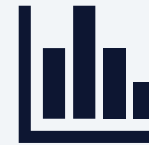
Breach of Law



Recording



Assessing



Reporting

Communicate

- If it is known that a member will not get a statement by 31 March 2025 they need to be told they will not be getting a statement.
Members do not need an individual reason or a category (ie section 29 or breach) although it is ideal.
- Members should however be informed about the timescales of when they can expect to receive an RSS.

Extend relevant date

- Scheme managers will need to have made a section 29 decision or not on a class or classes of members **before** 31 March 2025.
That means their governance process will need to show for example how they have categorised a class of member our factsheet shows what types of members could be categorised as section 29 decisions- [Why-might-an-RSS-be-delayed.pdf](#).
It is enough for a force to determine that members who fit these categories will have an extended relevant date.

Breach

- Where it has been determined a breach will occur and not a section 29 extension the force will need to record the breach. This is done internally.
- The next step will be to assess the breach for materiality. You should bring the assessment of materiality to your next pension board meeting.
- If the breach is deemed material it should be reported to the regulator.

Breach of Law – Responsibility

Everyone who is involved with governing, managing or administering the Police or Fire Pension Scheme has a responsibility to report breaches of law, or where the failure to comply is likely to be of material significance to The Pension Regulator.

The list of those responsible is not limited, but includes:

- **Managers of the Scheme**
- Pension Board members
- Any person involved with the administration of the scheme
- Employers
- Professional advisers including auditors, actuaries, legal advisers and fund managers
- Any other person involved in advising the scheme manager in relation to the scheme

Remedy – Breach of law

Rolled back ABS not sent by 31 August 2024

- The PSPJO Act 2022 [section 2](#) requires a member to have been treated as not and never have had service under the reformed scheme
- A rolled back ABS means that the ABS shows the member as being in the relevant legacy scheme for the remedy period.
- A non-rolled back ABS is an ABS that shows the member in the reform scheme during the remedy period.

An RSS not issued by the 'relevant date'

- Relevant date is set by [PSPJO Act 2022 section 29](#)
 - 31 March 2025, or
 - A later date set by the scheme manager.

Recording



There should be an established process to go through to collate all the necessary information to ensure that the potential or actual breach can be properly escalated enabling the breach to be assessed, recorded and reported.



There should be a clear record of the breach, and this should be reported to the Local Pension Board in all cases, regardless of whether the breach was assessed as needing to be reported to The Pension Regulator or not.



Previous records of breaches may well have an impact on the decision to report to The Pension Regulator.



Each breach should be recorded on the record of assessment form and retained by the Scheme Manager.

Assessment

Detailed examples of red, amber and green breaches can be found on The Pension Regulator web pages under the [assess whether to report a breach of pension law](#) section.

A breach is reportable as a red breach where one or more of the following applies:

- it was caused by dishonesty, negligence, reckless behaviour, poor scheme governance, ineffective controls resulting in deficient administration, or slow or inappropriate decision-making practices, poor advice, or intentionally breaking the law
- its effect is significant
- inadequate steps are being taken to put matters right
- it has wider implications

Assessing



An assessment needs to be carried out in the first instance as soon as possible after a breach has occurred, before it can be decided what course of action should be taken.



You will need to collate all relevant information, including what led you to this point, what actions have so far been taken, what internal controls were in place, a clear explanation of what has happened and how the breach has been identified.



To assess the breach, you will need to determine: –

- The cause of the breach
- The effect of the breach
- The reaction to the breach
- The wider implications of the breach

Assessment

| | Red (always reported) | Amber (sometimes reported) | Green (not reported) |
|--------------------|---|--|---|
| Cause | <p>Poor scheme governance or ineffective internal controls resulting in</p> <ul style="list-style-type: none"> • Deficient administration, • Slow or inappropriate decision making practices, • Poor advice, • Negligence | <p>Does not obviously fall into red or green classification.</p> <p>Consideration will need to be given to cause, effect and wider implications.</p> | <p>Was not caused by Poor scheme governance, Poor advice, Poor decision making</p> |
| Effect | Significant | <p>Previous breaches and mitigating actions may be relevant to determine material significance.</p> | |
| Reaction | Inadequate steps are being taken to put matters right | | Steps are being taken to put matters right (timeframes given) |
| Wider Implications | Significant | | |

Assessment considerations

The cause of the breach

- Possible causes to consider?
 - Lack of planning
 - Lack of control
 - Lack of data
 - Lack of knowledge and understanding
 - Lack of governance
 - Lack of contract management

The effect of the breach

- Possible effects
 - Lack of knowledge and expectation about what an RSS is?
 - Lack of cohort analysis on vulnerable or detrimented members
 - Knowledge on effect of protected members

The reaction to the breach

- What is being done to put matters right?
- What mitigation and governance has been in place to manage the breach.
- Was it expected?

The wider implications of the breach

- Lack of controls
- Reputational damage
- Lack of contract management
- Knowledge management and gaps
- Legal action

- Action
 - What action are you going to take?
- History
 - Has this breach or similar breaches occurred before?
 - What did you do to prevent a similar breach occurring
 - Did you report a breach of ABS in August, if you did not, but did not provide a rolled back ABS why did you not report a breach?

Common remedy challenges

Data not available

- You will need to consider what actions you took to prepare, did you start early when advised to
- Did you take on extra resource
- Were your SLT aware of the data challenges you had?
- Was this being monitored by your pension board

GAD guidance on divorce and transfers in not available

- Do you have any mitigation available
- Is this likely to occur again?

Reporting

10

Where it is deemed that a breach should be reported to The Pension Regulator as soon as reasonably practicable, ideally this should be within 10 working days of the breach being identified or having occurred.



Reporting breaches to The Pension Regulator is done online via the [Exchange](https://login.thepensionsregulator.gov.uk/) (<https://login.thepensionsregulator.gov.uk/>) service where you are already associated with a Police Pension Scheme by going to the “My Schemes” option. If you are not associated with a scheme you will need to select the “Share limited information with us about a registered scheme” option to report the breach.

Guidance

Police – Breach guidance and assessment template

Fire – Breach guidance and Assessment template

Disclaimer

The information contained in these slides are the authors interpretation of the current regulations.

Readers should take their own legal advice on the interpretation of any particular piece of legislation.

No responsibility whatsoever will be assumed by NPCC for any direct or consequential loss, financial or otherwise, damage or inconvenience, or any other obligation or liability incurred by readers relying on information contained in these slides.