SOUTH YORKSHIRE
PENSIONS AUTHORITY

Reporting Breaches Procedure

Draft - v. 2019.01to incorporate personal data breaches

1. Introduction

1.1 This document sets out the procedures to be followed by certain persons involved with the South Yorkshire Pensions Authority, the Local Government Pension Scheme managed and administered by South Yorkshire Pensions Authority, in reporting breaches of the law to the Pensions Regulator. It has been updated and extended to include the procedure to be followed when a personal data breach occurs which involves actual or potential failure to meet the requirements of the Data Protection Act, General Data Protection Regulation (GDPR) and/or common law duty of confidentiality. It is recognised that there may be an overlap between personal data breaches under GDPR and breaches of law in relation to the LGPS.

1.2 Breaches, personal data breaches and security incidents, can occur in relation to a wide variety of the tasks normally associated with the administrative function of a scheme such as keeping records, internal controls, calculating benefits and making investment or investment-related decisions.

1.3 This Procedure document applies in the main to:

- All members of the South Yorkshire Pensions Authority
- All members of the South Yorkshire Local Pension Board.
- All officers involved in the management of the Pension Fund including the Pensions Administration Team, the Investment Team and the Treasurer (Section 151 Officer).
- Any professional advisors including auditors, actuaries, legal advisors and fund managers.
- Officers of employers participating in South Yorkshire Pension Fund who are responsible for Local Government Pension Scheme matters.

2. Requirements

2.1 This section clarifies the extent of the legal requirements and to whom they apply.

2.2 Pensions Act 2004

Section 70 of the Pensions Act 2004 (the Act) imposes a requirement on the following persons:

- A trustee or manager of an occupational or personal pension scheme;
- A member of the Pension Board of a public service pensions scheme (in the case of South Yorkshire, the Authority and the Local Pension Board);
- A person who is otherwise involved in the administration of an occupational or personal pension scheme;
- The employer in relation to an occupational pension scheme;
- A professional advisor who is otherwise involved in advising the trustees of managers of an occupational or personal pension scheme in relation to the scheme.

To report a matter to the Pensions Regulator as soon as it becomes practicably possible where that person has reasonable cause to believe that:

a) a legal duty relating to the administration of the scheme has not been or is not being complied with, and

b) the failure to comply is likely to be of material significance to the Regulator.

The Act states that a person can be subject to a civil penalty if he or she fails to comply with this requirement without a reasonable excuse. The duty to report breaches under the Act overrides any other duties the individuals listed above may have. However, the duty to report does not override 'legal privilege'. This means that, generally, communications between a professional legal advisor and their client, or a person representing their client, in connection with legal advice being given to the client, do not have to be disclosed.

2.3 General Data Protection Regulation

GDPR defines a personal data breach as: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." Destruction is where the data no longer exists, or no longer exists in a form that is of any use to the controller. Damage is where personal data has been altered, corrupted, or is no longer complete. In terms of "loss" of personal data, this should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession. Finally, unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals. This highlights the difference between a security incident and a personal data breach – in essence, whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches.

Types of personal data breaches

- Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
- Integrity breach - where there is an unauthorised or accidental alteration of personal data.

It should also be noted that, depending on the circumstances, a breach can concern confidentiality, availability and integrity of personal data at the same time, as well as any combination of these.

2.4 The Pension Regulator's Code of Practice

Practical guidance in relation to this legal requirement is included in The Pension Regulator's Code of Practice in the following areas:

- Implementing adequate procedures.
- Judging whether a breach must be reported.
- Submitting a report to the Pensions Regulator.
- Whistleblowing protection and confidentiality.

2.4 Application to the South Yorkshire Pension Fund

This procedure has been developed to reflect the guidance contained in the Pension Regulator's Code of Practice in relation to the South Yorkshire Pension Fund and this document sets out how the Authority will strive to achieve best practice through use of a formal reporting breaches procedure.

3. The South Yorkshire Pension Fund Reporting Breaches Procedure

The following procedure details how individuals responsible for reporting and whistleblowing can identify, assess and report (or record if not reported) a breach of the law or a personal data breach relating to the South Yorkshire Pension Fund. It aims to ensure individuals responsible are able to meet their legal obligations and avoid placing any reliance on others to report. The procedure will also assist in providing an early warning of possible malpractice and reduce risk.

3.1 Clarification of the law

Individuals may need to refer to regulations and guidance when considering whether or not to report a possible breach. Some of the key provisions are shown below:

- Section 70(1) and 70(2) of the Pensions Act 2004
- Employment Rights Act 1996
- Occupational and Personal Pension Schemes (Disclosure of Information) Regulations 2013 (Disclosure Regulations)
- Public Service Pension Schemes Act 2013
- Local Government Pension Scheme Regulations Pre 2014 schemes 2014 scheme

  General Data Protection Regulation

- The Pension Regulator's Code of Practice

In particular, individuals should refer to the section on 'Reporting Breaches of the Law' and for information about reporting late payments of employee or employer contributions refer to the section on 'Maintaining Contributions'

Further guidance and assistance can be provided by the Treasurer (s151 Officer) and the Monitoring Officer, provided that requesting this assistance will not result in alerting those responsible for any serious offence (where the breach is in relation to such an offence).

3.2 Clarification when a breach is suspected

Individuals need to have reasonable cause to believe that a breach has occurred, not just a suspicion. Where a breach is suspected, the individual should carry out further checks to confirm the breach has occurred. Where the individual does not know the facts or events, it will usually be appropriate to check with the Treasurer, the Monitoring Officer, a member of the Pensions Authority or Local Pension Board or others who are able to explain what has happened. However, there are some instances where it would not be appropriate to make further checks, for example, if the individual has become aware of theft, suspected fraud or another serious offence and they are also aware that by making further checks there is a risk of either alerting those involved or hampering the actions of the police or a regulatory authority. In these cases the Pensions Regulator should be contacted without delay.

3.3 Determining whether the breach is likely to be of material significance

To decide whether a breach is likely to be of material significance an individual should consider the following, both separately and collectively:

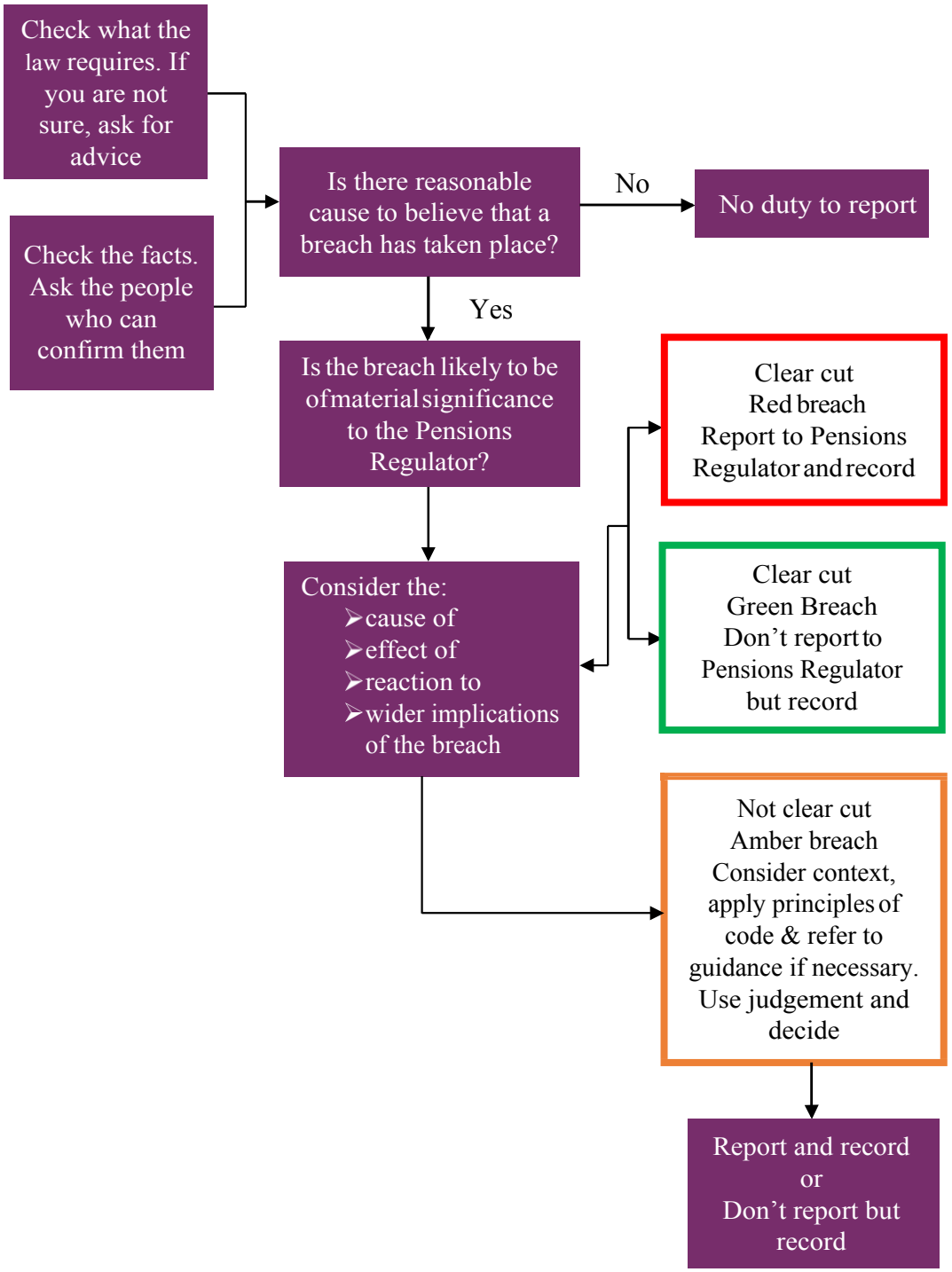
- Cause of the breach (what made it happen).
- Effect of the breach (the consequence(s) of the
- breach). Reaction to the breach.
- Wider implications of the breach.

Further details on the above four considerations are provided in Appendix A to this procedure.

The individual should use the traffic light framework described in Appendix B to help assess the material significance of each breach and to formally support and document their decision.

3.4 A decision tree is provided below to show the process for deciding whether or not a breach has taken place and whether it is materially significant and therefore requires to be reported. In relation to personal data breaches identified by officers of the Authority it is expected that all breaches will be recorded on the breach management log and a member of the SYPA Senior Management Team will determine whether an immediate report is required to the Pensions Regulator or to the Data Protection Officer/Information Commissioner's Office.

Decision-tree: deciding whether to report



3.5 Referral to a level of seniority for a decision to be made on whether to report

South Yorkshire Pensions Authority has a designated Monitoring Officer to ensure the Authority acts and operates within the law. They are considered to have appropriate experience to help investigate whether there is reasonable cause to believe a breach has occurred, to check the law and facts of the case, to maintain records of all breaches and to assist in any reporting to the Pensions Regulator, where appropriate. If breaches relate to late or incorrect payment of contributions or pension benefits, the matter should be highlighted to the Monitoring Officer and the Treasurer at the earliest opportunity to ensure the matter is resolved as a matter of urgency. Individuals must bear in mind, however, that the involvement of the Monitoring Officer is to help clarify the potential reporter's thought process and to ensure this procedure is followed. The reporter remains responsible for the final decision as to whether a matter should be reported to the Pensions Regulator.

The matter should not be referred to any of these officers if doing so will alert any person responsible for a possible serious offence to the investigation (as highlighted in section 2). If that is the case, the individual should report the matter to the Pensions Regulator setting out the reasons for reporting, including any uncertainty – a telephone to the Regulator before the submission may be appropriate, particularly in more serious breaches.

3.6 Dealing with complex cases

The Treasurer or Monitoring Officer may be able to provide guidance on particularly complex cases. Information may also be available from national resources such as the Scheme Advisory Board or the LGPC Secretariat (part of the LGA Group). If timescales allow, legal advice or other professional advice can be sought and the case can be discussed at the next Authority meeting.

3.7 Timescales for reporting

The Pensions Act and Pension Regulators Code require that if an individual decides to report a breach, the report must be made in writing as soon as reasonably practicable. Individuals should not rely on waiting for others to report and nor is it necessary for a reporter to gather all the evidence which the Pensions Regulator may require before taking action. A delay in reporting may exacerbate or increase the risk of the breach. The time taken to reach the judgements on "reasonable cause to believe" and on "material significance" should be consistent with the speed implied by 'as soon as reasonably practicable'. In particular, the time taken should reflect the seriousness of the suspected breach.

Specifically in relation to personal data breaches, an officer should inform their line manager immediately who will update the breach reporting system. This prompts a notification to be sent to the Head of Pensions Administration who will investigate whether the breach needs to be notified to the Data Protection Officer.

3.8 Early identification of very serious breaches

In cases of immediate risk to the scheme, for instance, where there is any indication of dishonesty, the Pensions Regulator does not expect reporters to seek an explanation or to assess the effectiveness of the 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 Pensions Regulator to the breach.

If an officer suspects a serious breach of personal data, they may immediately report this directly to the Data Protection Officer. The contact details for the Data Protection Officer are available on SharePoint via the Breach Reporting link on the home page.

3.9 Recording all breaches even if they are not reported

The record of past breaches may be relevant in deciding whether to report a breach, for example, it may reveal a systemic issue. South Yorkshire Pensions Authority will maintain a record of all breaches identified by individuals and managers should ensure that the breach reporting log is updated immediately in all cases. Records of unreported breaches should also be provided as soon as reasonably practicable and certainly no later than within 20 working days of the decision not to report. These will be recorded alongside all reported breaches. The record of all breaches (reported or otherwise) will be reported to the Local Pensions Board on a quarterly basis and this will also be shared with the Pensions Authority.

3.10 Reporting a breach to the Regulator

Reports must be submitted in writing via the Pensions Regulator's online system, or by post, email or fax, and should be marked urgent if appropriate. If necessary, a written report can be preceded by a telephone call. Reporters should ensure they receive an acknowledgement for any report they sent to the Pensions Regulator. The Pensions Regulator will acknowledge receipt of all reports within five working days and may contact reporters to request further information. Reporters will not usually be informed of any actions taken by the Pensions Regulator due to restrictions on the disclosure of information.

As a minimum, individuals reporting should provide:

- Full scheme name (South Yorkshire Pensions Authority).
- Description of breach(es).
- Any relevant dates.
- Name, position and contact details.
- Role in connection to the scheme.
- Employer name or name of scheme manager (the latter is South Yorkshire Pensions Authority).

If possible, reporters should also indicate:

- The reason why the breach is thought to be of material significance to the Pensions Regulator.
- Scheme address (provided at the end of this procedure document)
- Scheme manager contact details (provided at the end of this procedure document).
- Pension Scheme registry number (10165252).
- Whether the breach has been reported before.

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

3.11 Confidentiality

If requested, the Pensions Regulator will do its best to protect a reporter's identity and will not disclose information except where it is lawfully required to do so. If an individuals' employer decides not to report and the individual employed by them disagrees with this and decides to report a breach themselves, they may have protection under the Employment Rights Act 1996 if they make an individual report in good faith.

3.12 Reporting to South Yorkshire Pensions Authority and the Local Pension Board

A report will be presented to the Pensions Authority and the Local Pension Board on a quarterly basis setting out:

- All breaches, including those reported to the Pensions Regulator and those unreported, with associated dates.
- In relation to each breach, details of what action was taken and the result of any action (where not confidential).
- Any future actions for the prevention of the breach in question being repeated.
- Highlighting new breaches which have arisen in the last year/since the previous meeting.

This information will also be provided upon request by any other individual or organisation (excluding sensitive/confidential cases or ongoing cases where discussion may influence the proceedings).

Review

This Reporting Breaches Procedure will be kept under review and updated as considered appropriate by the Treasurer. It may be changed as a result of legal or regulatory changes, evolving best practice and ongoing review of the effectiveness of the procedure.

Further information

If you require further information about reporting breaches or this procedure, please contact:

Jason Bailey – Head of Pensions
Administration Email: JBailey@sypa.org.uk

Telephone: 01226 772954

George Graham – Fund Director
Email: GGraham@sypa.org.uk

Telephone: 01226 772887

Designated officer contact details:

Treasurer – Neil Copley
Email: neilcopley@barnsley.gov.uk

Telephone: 01227 773237

Monitoring Officer – Andrew Frosdick
Email: andrewfrosdick@barnsley.gov.uk

Telephone: 01226 773001

APPENDIX A

Determining whether a breach is likely to be of material significance.

To decide whether a breach is likely to be of material significance individuals should consider the following elements, both separately and collectively:

- Cause of the breach (what made it happen).
- Effect of the breach (the consequence(s) of the breach).
- Reaction to the breach.
- Wider implications of the breach.

The cause of the breach

Examples of causes which are likely to be of concern to the Pensions Regulator are provided below:

- Action, or failing to act, in deliberate contravention of the law.
- Incomplete or inaccurate advice.
- Poor administration, i.e. failure to implement adequate administration procedures.
- Poor governance.
- Slow or inappropriate decision-making practices.

When deciding whether a cause is likely to be of material significance individuals should also consider:

- Whether the breach has been caused by an isolated incident such as a power outage, fire, flood or a genuine one-off mistake.
- Whether there have been any other breaches (reported to the Pensions Regulator or not) which when taken together may become materially significant.

The effect of the breach

Examples of possible effects (with possible causes) of breaches which are considered likely to be of material significance to the Pensions Regulator in the context of the LGPS are given below:

- Authority/Board members not having enough knowledge and understanding, resulting in the Authority and Boards not fulfilling their roles, the scheme not being properly governed and administered and/or scheme managers breaching other legal requirements.
- Conflicts of interest of Authority or Board members, resulting in them being prejudiced in the way they carry out their role and/or the ineffective governance and administration of the scheme and/or scheme managers breaching legal requirements.
- Poor internal controls, leading to schemes not being run in accordance with their scheme regulations and other legal requirements, risks not being properly identified and managed and/or the right money not being paid to or by the scheme at the right time.

- Inaccurate or incomplete information about benefits and scheme information provided to members, resulting in members not being able to effectively plan or make decisions about their retirement.
- Poor member records held, resulting in member benefits being calculated incorrectly and/or not being paid to the right person at the right time.
- Misappropriation of assets, resulting in scheme assets not being safeguarded.
- Other breaches which result in the scheme being poorly governed, managed or administered.

The reaction to the breach

A breach is likely to be of concern and material significance to the Pensions 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.

The wider implications of the breach

Reporters should also consider the wider implications when deciding whether a breach must be reported. The breach is likely to be of material significance to the Pensions Regulator where the fact that a breach has occurred makes it more likely that further breaches will occur within the Fund or, if due to maladministration by a third party, further breaches will occur in other pension schemes.

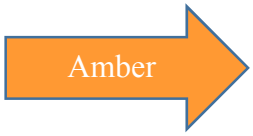
Traffic light framework for deciding whether or not to report

It is recommended that those responsible for reporting use the traffic light framework when deciding whether to report to the Pensions Regulator. This is illustrated below:

Where the cause, effect, reaction and wider implications of a breach, when considered together, are likely to be of material significance.

These must be reported to the Pensions Regulator.

Example: Several members' benefits have been calculated incorrectly. The errors have not been recognised and no action has been taken to identify and tackle the cause or to correct the errors.



Where the cause, effect, reaction and wider implications of a breach, when considered together, may be of material significance. They might consist of several failures of administration that, although not significant in themselves, have a cumulative significance because steps have not been taken to put things right. You will need to exercise your own judgement to determine whether the breach is likely to be of material significance and should be reported.

Example: Several members' benefits have been calculated incorrectly. The errors have been corrected, with no financial detriment to the members. However, the breach was caused by a system error which may have wider implication for other public service schemes using the same system.

Where the cause, effect, reaction and wider implications of a breach, when considered together are not likely to be of material significance. These should be recorded but do not need to be reported.

Example: A members' benefits have been calculated incorrectly. This was an isolated incident, which has been promptly identified and corrected, with no financial detriment to the member. Procedures have been put in place to mitigate against this happening again.

All breaches should be recorded even if the decision is not to report.

When using the traffic light framework, individuals should consider the content of the red, amber and green sections for each of the cause, effect, reaction and wider implications of the breach, before you consider the four together. Some useful examples of this framework is provided by the Pensions Regulator