



# Breaches Policy

March 2026

# Contents

Introduction .....	2
Purpose of the Breaches Policy & Procedure .....	2
Legal Requirements .....	2
Pensions Act 2004 .....	2
The Pension Regulator's General Code of Practice (GCoP) .....	3
The UK General Data Protection Regulation (UK GDPR) .....	3
Types of breaches .....	3
Data breaches .....	3
TPR's GCoP breaches .....	4
Roles and responsibilities .....	4
Notification of a breach to the Fund .....	6
Procedure for reporting breaches .....	6
Check there is reasonable cause to report a breach .....	6
Determine whether the breach is of material significance .....	7
Take swift action.....	7
Report a General Code of Practice breach to the Pension Regulator .....	7
Report a data breach to the Information Commissioner (ICO) .....	8
Recording of breaches.....	8
Reporting to Local Pension Board and Pension Fund Committee .....	8
Review .....	9
Appendix A.....	10
Appendix B.....	11

## Introduction

This document sets out the policy and procedures to be followed by the various parties involved with the Lancashire County Pension Fund in relation to identifying and reporting breaches of the law to the Pensions Regulator (tPR) or Information Commissioner's Office (ICO).

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

**Definition of a breach** – where a legal duty relating to the administration of the scheme has not been or is not being complied with.

This document applies to the Lancashire County Pension Fund (The Fund). The Fund is part of the Local Government Pension Scheme (LGPS) managed and administered by Lancashire County Council.

## Purpose of the Breaches Policy & Procedure

This document has been developed to reflect guidance contained in the Pension Regulator's General Code of Practice (GCoP) and to reflect the duty on all organisations to report certain personal data breaches in line with the UK General Data Protection Regulations (GDPR). The document sets out how the Fund will strive to achieve best practice through use of a formal breaches reporting procedure.

The purpose of the policy is –

- to ensure that those with a responsibility to report breaches understand their legal obligations, and
- to outline how the Fund will strive to achieve best practice through use of a formal breaches reporting procedure.

The purpose of the procedure is –

- to provide details on how individuals responsible for reporting and whistleblowing can identify, assess and report (or record if not reported) a breach of law relating to the Fund.
- to ensure individuals responsible can 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.

## Legal Requirements

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

### **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 pension scheme.
- 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 adviser in relation to such a scheme.
- a person who is otherwise involved in advising the trustees or managers of an occupational or personal pension scheme in relation to the scheme.
- a scheme strategist or scheme funder of a Master Trust scheme within the meaning of Part 1 of the Pension Schemes Act 2017 (see section 39 of that Act).

Where the person has reasonable cause to believe that—

- a) a duty which is relevant to the administration of the scheme in question, and is imposed by or by virtue of an enactment or rule of law, 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 in the exercise of any of its functions,

they must give a written report of the matter to the Regulator as soon as reasonably practicable.

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. As per tPR's GCoP, 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 adviser 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.

### **The Pension Regulator's General Code of Practice (GCoP)**

Practical guidance in relation to this legal requirement is included in The Pension Regulator's General Code of Practice, published on the [Pension Regulator's website](#) and covers the following areas:

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

### **The UK General Data Protection Regulation (UK GDPR)**

In accordance with the UK GDPR, personal data must be processed in line with these fundamental principles:

- Processed lawfully, fairly and in a transparent manner (we must have a legal basis for processing and tell the data subject what we are doing with their data via a privacy notice)
- Processed for specified, explicit and legitimate purposes (we can't collect it for one reason and use it for another)
- Adequate, relevant and limited to the purposes for which we collected it (we can't collect more than we need)
- Accurate and up to date (we have to ensure data quality)
- Not kept longer than is necessary (we need to set data retention periods)
- Processed in a manner that ensures security (we need to use technical and organisational controls to ensure the security of personal data)

Art. 4 (12) UK 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"*.

## **Types of breaches**

There are two types of breaches outlined below-

### **Data breaches**

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 and deliberate causes. It also means that a breach is more than just about losing personal data.

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

### **TPR's GCoP breaches**

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

#### **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.

Performance of scheme employers is monitored against the standards set out in the [Pension Administration Strategy Statement](#).

#### **Maintaining contributions**

Contribution breaches occur when an employer fails to make a timely payment or consistently pays an incorrect amount. The latter will usually occur when an employer has failed to submit a remittance advice, and an incorrect amount has therefore been collected. Consistently is considered to be on four separate occasions in a 12-month period.

Collection of contributions is monitored on a monthly basis and payment failures are categorised and managed as follows -

**Incident** – an incorrect amount is collected/no remittance provided (first, second or third occasion). These are dealt with in line with the Fund's 'Contribution Escalation Policy'.

**Breach** – an incorrect amount collected on four or more occasions, **or** any payment is late. These are dealt with in line with the Fund's 'Contribution Escalation Policy'.

#### **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](#).

## **Roles and responsibilities**

The table below outlines the key parties involved in the reporting and managing of breaches. Individuals can report breaches to the Pensions Regulator or ICO directly. However, there is a process that allows the Fund to actively manage the monitoring and reporting of breaches which is outlined in this document.

Local Pensions Partnership Investment Limited (LPPI) and Local Pensions Partnership Administration Limited (LPPA) <sup>1</sup>	<ul style="list-style-type: none"><li>• comply with all obligations under Data Protection Laws, and in the event of any security breach, they are required to report the matter to the Administering Authority immediately upon becoming aware of the breach</li><li>• must comply with the requirements of the Pension Regulator's General Code of Practice and any contractual agreements. Any suspected breaches are to be immediately flagged to the Administering Authority, with a full report submitted within 5 working days of the incident first being identified</li><li>• report any breaches to the Fund's Governance team or Lancashire County Council's (LCC) Information Governance Team</li></ul>
--	--

<sup>1</sup> LPPA and LPPI provide pensions administration services and pooled investment services to the Pension Fund. LPPI also manage all non-pooled investments.

Fund Finance team	<ul style="list-style-type: none"> <li>• ensure employer contributions are collected each month from scheme employers</li> <li>• report any contribution breaches to the Fund's Governance team</li> <li>• manage any contribution incidents and breaches</li> </ul>
LCC Information Governance Team	<ul style="list-style-type: none"> <li>• manage information security incidents in line with LCC <a href="#">Information security incident management policy</a></li> <li>• investigate and manage all Fund related data breaches, liaising with the Fund as required.</li> <li>• forward a copy of the eForm notification directly to the Fund mailbox (<a href="mailto:LCPFBreaches@lancashire.gov.uk">LCPFBreaches@lancashire.gov.uk</a>)</li> <li>• provide technical advice and support to the Fund as required about their legal obligations and to ensure that any processing of personal data by the council is lawful</li> </ul>
Fund Governance Team	<ul style="list-style-type: none"> <li>• monitor data breaches and work with the LCC Information Governance team as required to support their investigations</li> <li>• Investigate all General Code of Practice breaches. All breaches will be reported as necessary to the Head of Fund</li> <li>• ensure that the reporter is kept updated on the progress of any investigation. If a decision is taken not to report the breach, and the reporter is not satisfied with that outcome, the reporter retains the option to report the breach directly to the Pension Regulator or Information Commissioner's Office</li> </ul>
Head of Fund	<ul style="list-style-type: none"> <li>• make the final decision regarding reporting of a breach to either the Pension Regulator or Information Commissioner's Office</li> <li>• consult with LCC's Senior Information Risk Owner (SIRO) or Data Protection Officer regarding their decision to report any data breaches</li> </ul>
Pension Fund Committee Members, Local Pension Board Members and Fund Officers	<ul style="list-style-type: none"> <li>• responsibility to report breaches</li> </ul>

A suspected breach should not be referred to any individual if doing so will alert any person responsible for a possible serious offence to the investigation. If that is the case, the individual should report the matter directly to The Pensions Regulator or Information Commissioner as appropriate, setting out the reasons for reporting, including any uncertainty – a telephone call to the Regulator or Information Commissioner before the submission may be appropriate, particularly in more serious breaches.

## Notification of a breach to the Fund

All suspected/actual breaches should be reported to the Fund at the earliest opportunity to ensure the matter is resolved as a matter of urgency.

Any data breaches should be reported to the LCC Information Governance Team through the completion of an eform on the LCC website – '[Information Security Incident Reporting Form](#)'. These will be investigated by LCC's Information Governance team and reported to the Fund Governance team for monitoring purposes. In practice, LPPA will mainly report data breaches, and this is done by a bespoke data breach reporting form. However, it is possible that other parties could report via the online eform.

Any breaches relating to the TPR's GCoP, including contribution breaches should be reported to the Fund Governance team through completion of '[LCPF Breaches Reporting eForm](#)' on the LCC website and will be received directly for investigation by the Fund Governance team. In practice, LPPA will mainly report GCoP breaches, and the Fund Finance team will report contribution breaches.

However, it is possible that other parties could report.

The 'reporter' must provide the date of the incident, a description of the suspected breach, the potential impact on operations or the individual and whether they believe the breach is of material significance, among other key details listed on the reporting forms.

## Procedure for reporting breaches

This section outlines the procedure to follow when a breach is reported to the Fund or LCC Information Governance Team including the process for reporting to the Pension Regulator or Information Commissioner (ICO). This is summarised in 'Appendix A'.

### **Check there is reasonable cause to report a breach**

Individuals need to have reasonable cause to believe that a breach has occurred, not just a suspicion. Where a breach is suspected, the individual may need to refer to regulations and guidance when considering whether or not to report a possible breach. Some of the key provisions are listed below:

Section 70(1) and 70(2) of the Pensions Act 2004: [www.legislation.gov.uk/ukpga/2004/35/contents](http://www.legislation.gov.uk/ukpga/2004/35/contents)

Employment Rights Act 1996: [www.legislation.gov.uk/ukpga/1996/18/contents](http://www.legislation.gov.uk/ukpga/1996/18/contents)

Occupational and Personal Pension Schemes (Disclosure of Information) Regulations 2013: [www.legislation.gov.uk/uksi/2013/2734/contents/made](http://www.legislation.gov.uk/uksi/2013/2734/contents/made)

Public Service Pensions Act 2013: [www.legislation.gov.uk/ukpga/2013/25/contents](http://www.legislation.gov.uk/ukpga/2013/25/contents)

Local Government Pension Scheme Regulations (various):

[LGPS Regulations 2013 \(pre 2014 schemes\)](#)

[LGPS Transitional Regulations 2014 \(2014 scheme\)](#)

The Pensions Regulator's General Code of Practice: [Code of practice](#)

In particular, individuals should refer to the section on 'Reporting to TPR.'

The UK General Data Protection Regulations (GDPR): [Guide to the UK General Data Protection Regulation \(UK GDPR\) | ICO](#)

Further guidance and assistance can be provided by the Director of Law and Governance in carrying out any immediate or necessary checks, provided that in carrying out such checks those implicated in any potential breach are not alerted. This is highly unlikely given that the Director of Law and Governance, whilst an officer of the County Council, is largely independent from the Fund and its day-to-day operations. Where there is any doubt reporters should contact The Pensions Regulator or Information Commissioner direct.

The Director of Law and Governance 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 - <http://www.lgpsregs.org/>). If timescales allow, legal advice or

other professional advice can be sought, and the case can be discussed at the next available Local Pension Board meeting.

Where the individual does not know the facts or events, they should raise their concerns as soon as possible with the Fund Governance Team. 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.

### **Determine whether the breach is of material significance**

As per the General Code of Practice guidance, the determination of whether a breach is likely to be of material significance should be considered. Each of the following should be considered 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.

A decision tree from the Pension Regulators website helps to set out the process for considering whether or not a breach has taken place and whether it is materially significant and therefore requires to be reported.

This can be found at 'Appendix B'. More detailed guidance can be accessed from the link below:

[Pensions Regulator – Complying with the duty to report breaches of the law](#)

In respect of a data breach, you should consider the likelihood and severity of the risk to people's rights and freedoms, following the breach.

### **Take swift action**

The Pensions Act and Pension Regulators General Code of Practice 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.

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 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 Pensions Regulator to the breach.

In respect of personal data breaches these should be reported to the Information Commissioner without undue delay (if it meets the threshold for reporting) and within 72 hours.

### **Report a General Code of Practice breach to the Pension Regulator**

Reports must be submitted in writing via tPR's [website, or by post, email](#), 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 send 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.

Further guidance on reporting to TPR can be found within the [General Code of Practice](#).

## **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 individual's 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.

## **Report a data breach to the Information Commissioner (ICO)**

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.

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. Further guidance regarding how to respond to a personal data breach can be found here [72 hours - how to respond to a personal data breach | ICO](#)

Reports can be made by calling the Information Commissioner helpline on **0303 123 1113** or by completing an on-line Form. Further guidance can be found on the following webpage: [UK GDPR data breach reporting \(DPA 2018\) | ICO](#)

You will be required to provide details of what has happened, when and how you found out about the breach, the people that have or may have been affected, what you're doing in response and contact details in the event the ICO need more information.

## **Recording of breaches**

A record of the breaches will be retained by the Fund including details of breaches that don't require reporting to the Pension Regulator or Information Commissioner.

The record of past breaches may be relevant in deciding whether to report a future breach (for example it may reveal a systemic issue).

## **Reporting to Local Pension Board and Pension Fund Committee**

The Fund Governance Team will ensure that a report is presented to each meeting of the Local Pension Board setting out:

- All breaches, including those reported to the Pensions Regulator or Information Commissioner and those unreported.
- In relation to each breach, details of what action was taken and the result of any action.
- Any future actions for the prevention of the breach in question being repeated.

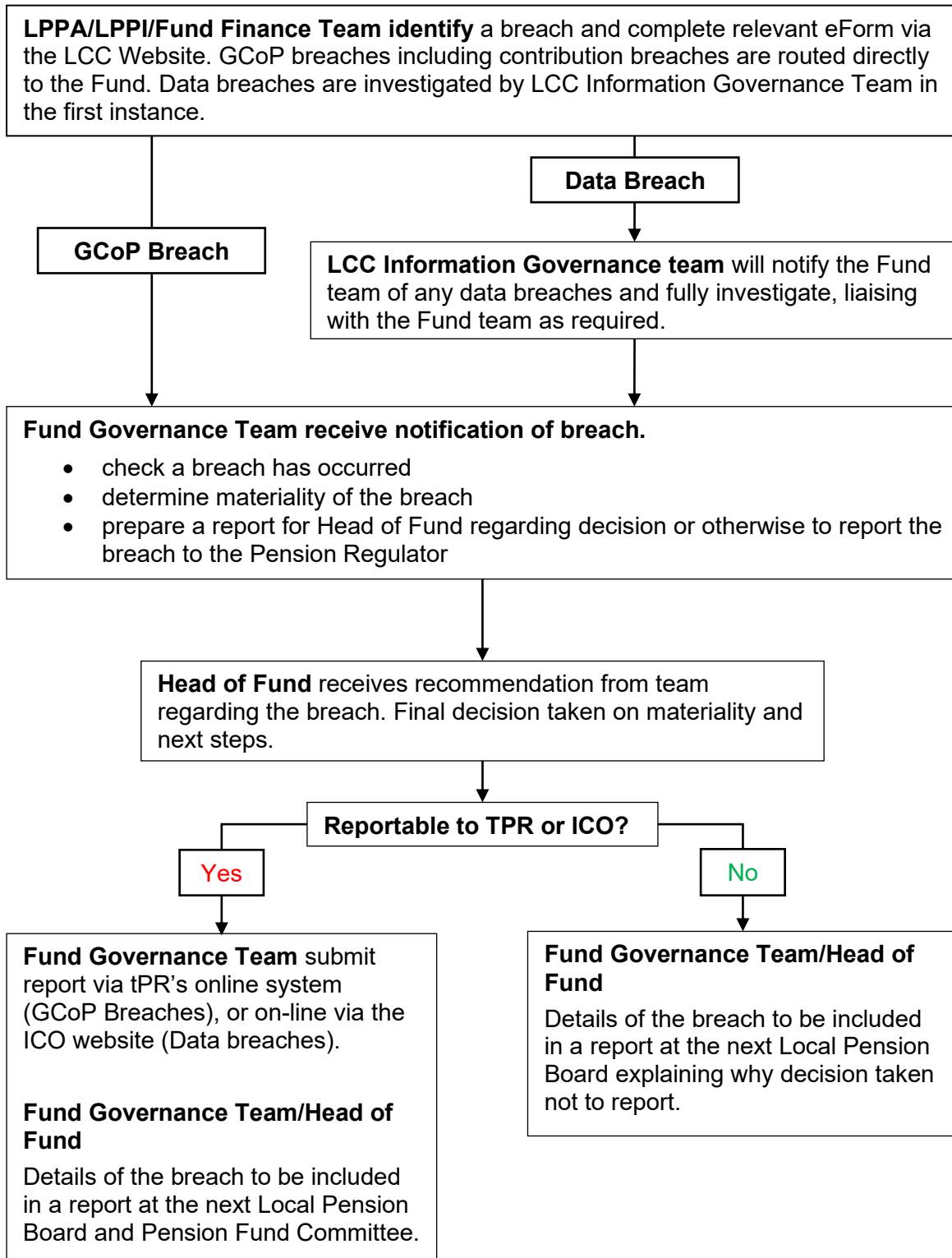
The Fund Governance Team will ensure that a summary report is presented each year to the Pension Fund Committee on breaches. In addition, if a breach is deemed reportable to the Pensions Regulator or Information Commissioner, the Pension Fund Committee will be informed of this at its nearest quarterly 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 policy and procedure will be kept under review and updated as considered appropriate by the Fund Governance Team, in consultation with the Head of Fund. It may be amended as a result of legal or regulatory changes, evolving best practice and ongoing review of the effectiveness of the procedure.

# Appendix A



# Appendix B

