**LPPA Breach Reporting**

|  |  |
| --- | --- |
| Authority & decision trail: | 1. **Decision Trail:** LCPF Local Pension Board   **Authority:** LPPA Senior Leadership Team |
| Lead Officers:  Report writers: | Janet Morville-Smith Head of Risk & Compliance, Pensions Administration  [janet.morville-smith@localpensionspartnership.org.uk](mailto:janet.morville-smith@localpensionspartnership.org.uk) |
| LPP Information Classification:  - Applies to The LPP Group | **Confidential** |

**Purpose**

This paper seeks to provide an overview of the process used to assess and rate administration breaches.

**Background**

An action was raised at the last Board meeting requesting LPPA to provide a paper to explain the process adopted for administration breaches.

**Summary**

Since the formation of the LPPA Risk & Compliance team in 2020, the breach process has been enhanced to capture and report on all breaches, not just data breaches. This process has 3 categories of breach as detailed below:

|  |  |  |
| --- | --- | --- |
| Data Breach | Code of Practice 14 Breach | LPPA Process Breach |
| This type of breach impacts on personal data | This type of breach impacts on the administration of a pension scheme that is covered under the Pensions Regulator’s CoP14 | This type of breach impacts on LPPA’s own Policies and Procedures |
| Examples:   * Disclosure of information to an unauthorised party * Inaccurate record keeping * Loss of or damage to data records | Examples:   * Inaccurate record keeping (e.g. service history / transactions etc.) * Contribution Payments * Disclosure Requirements (e.g. ABS / Retirement Options etc.) * IDRP not processed in time | Examples:   * Process not followed * Use of personal email / phone * Email sent to incorrect email address (where no personal data is included) |

*N.B. These examples are not exhaustive*

LPPA take all breaches extremely seriously. A breach leads to errors which need to be addressed. Upon notification of any breach the Risk & Compliance team log these on the Breach Register and investigate how the breach happened, ensure any corrective work has been completed, and engage with the individual who caused the breach and their direct line manager to put in place measures to prevent the breach reoccurring.

Where a Member has been directly affected, measures are taken to apologise and provide protection if deemed appropriate, for example CIFAS.