Parliamentary Contributory Pension Fund (PCPF)

PCPF Personal Data Breach Policy

Policy Name: PCPF Personal Data Breach Policy
Version: 1.2
Approved by: Gurpreet Bassi, Secretary to the Trustees
Date approved: 25/03/2024
Date effective from: 25/03/2024
Next Review Date: 25/03/2026

Who we are

This policy has been prepared by the Board of Trustees ("the Trustees") of the Parliamentary Contributory Pension Fund ("the Scheme"). As Trustees of the Scheme, we hold certain personal information (known as "Personal Data") about Scheme members and, where applicable, their dependants and beneficiaries. Personal Data is the information from which you can be identified and any personal information we hold or process in respect of you will be subject to certain protections. The Trustees are known as the "Data Controller" as we decide the purposes for and the means by which the Personal Data we collect and hold is Processed. Owing to the nature of their role, the Scheme actuary will be a joint Data Controller of Scheme Personal Data alongside the Trustees.

Purpose

This policy sets out the procedure to be followed to ensure an effective approach is in place for managing a personal data breach. The policy relates to all personal and special categories (sensitive) data held by the Scheme.

Security and Data-Related Policies

This policy should be read in conjunction with the following policies:

- Data Protection Policy
- Privacy Notice

These policies are also designed to protect personal data and can be found on the PCPF website.

Background

A personal data breach is when the data for which an organisation is responsible for suffers a security incident affecting the confidentiality, integrity or availability of personal data. There will be a personal data breach:

- whenever any personal data is accidentally 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.

Some examples of personal data breaches include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Responsibility

Gurpreet Bassi, as the Secretary to the Trustees, has overall responsibility for managing any data breach within the Scheme and is the dedicated point of contact for all personal data breaches.

Assessing and Reporting a breach

In the event of a personal data breach, the Secretariat will undertake an assessment of the breach, gathering information needed to complete the PCPF Personal Data Breach Log and consider both the severity of the potential or actual impact on individuals as a result of a breach, and the likelihood of this occurring. The process is set out in Appendix A. The Secretary will also assess whether the following persons/bodies/organisations need to be informed:

- **Individuals to which the data relates to**: The UK GDPR requires that we report a Personal Data Breach that is likely to result in a high risk to the rights and freedoms of individuals, directly to the individual concerned and without undue delay.

  Guidance from the Information Commissioner's Office (ICO) states that a "high risk" means: "the requirement to inform individuals is higher than for notifying the ICO."

  When contacting the individuals, the following information should be included:

  - the details of the main contact person whom the individual can contact for more information;
  - a description of the likely consequences of the personal data breach; and
  - a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

  Where possible, we will give individuals clear advice on the steps they need to take to protect themselves. This may include forcing a password reset; advising individuals to use strong passwords; or advising them to look out for fraudulent activities or phishing emails.

- **ICO**: We must report a Personal Data Breach to the Information Commissioner's Office without undue delay (and where feasible within 72 hours), unless the breach is unlikely to result in a risk to the rights and freedoms of the individual and we can demonstrate this.

  If a risk is likely, we must notify the ICO; if a risk is unlikely, it does not need to be reported but will need to be documented on the PCPF Personal Data Breach Log and the reason for not reporting it should be justified.

  A data breach can be reported to the ICO on the phone (0303 123 1113) or online (ICO.org.uk). The ICO's self assessment tool on their website can also be used to determine whether we need to report to the ICO.

  If reporting on the phone then the following information should be provided:

  - When and how the breach was discovered
  - the nature of the breach
  - categories of data
  - number of data records
  - number of people affected
  - name and contact details of DPO/PCPF Secretariat
  - likely consequences of the breach and action taken, including whether the data subjects have been informed about the breach.

  The online form can be used to report a breach if we are confident we have dealt with the breach properly; or if the breach is still being investigated; or if we are reporting outside of normal ICO opening hours (Monday to Friday between 9am and 5pm). The "Personal data breach reporting form" can be downloaded at the following webpage: Data Breach Reporting

  Once complete it should be sent back via email or post using the details on the form.

- **Trustees**: The Secretariat will notify the Trustees of all serious breaches (that require reporting to the ICO) by email circulation as soon as possible following a breach taking place. Information will be provided about the nature of the breach, the number of individuals impacted, the assessment of the impact on individuals and how and when the individuals and the ICO were informed. The PCPF Personal Data Breach Log will also be updated and brought to the next appropriate meeting for noting.

  In instances of breaches, that do not require reporting to the ICO, the Secretariat will complete the PCPF Personal Data Breach Log and notify the Chairman of the breach. The Chairman will decide whether the breach should be brought to the attention of the Trustees immediately, by email circulate, or whether to bring the matter to the next appropriate Trustee meeting for noting.

Taking measures to contain the breach

Once the severity of the impact of the breach on the affected individuals and the likelihood of this occurring has been assessed, and if it is found that the breach may impact on the rights and freedoms of the individuals affected then the following measures should also be considered in order to ensure that the breach is contained:

- Consider whether there are any other people who should be informed of the breach, such as Parliamentary Digital Service, who may be able to help with containing the breach;
- Assess if there are any other steps that can be taken to contain the breach and recover the loss of any Personal Data; and
- Consider whether it is necessary to contact other third parties such as the police.

Relevant/Third Parties

In the event that any Relevant Parties and/or Third Parties become aware of a Personal Data Breach:

- Under the GDPR, they are required to notify the PCPF without undue delay. It has therefore been agreed that third parties would report a breach to the Secretary to the Trustees within 24 hours or as soon as reasonably practicable, providing as much information as possible (including the nature and the consequences of the Personal Data Breach and any measures taken or proposed to mitigate any adverse effects).
- The Secretary to the Trustees will investigate the cause of the Personal Data Breach and assess the risk to individuals, as well as establishing whether any action needs to be taken to recover any losses and to limit the damage caused by the Personal Data Breach, as described above. Where appropriate, the Secretary will inform the data subjects and ICO, as described above and ensure that the Personal Data Breach is recorded/documented.

Annual assurance statements are sought by third parties who gather, control or process personal data on behalf of the PCPF, regarding their own cyber security measures.

Preventing future breaches

Once the data breach has been dealt with the Secretary to the Trustees will evaluate the effectiveness of the response to the Personal Data Breach and identify any amendments required to this Policy. A review will include:

- looking at what measures were in place when the breach occurred and if any new measures could be implemented to prevent any such breaches in the future;
- considering whether there is a need for staff training on data protection;
- recording the data breach in a log; and

- making any required updates to the data protection policies, ensuring that all staff (and/or third parties, if relevant) are aware of them.

Media approach

In the event of a serious breach the Secretariat take advice from the House's Media team on the most effective approach. Responses to media enquires would be signed off by the Secretary as usual. Any additional proactive statements to be issued would be approved by the Chairman, and circulated to Trustees by email once issued.

Updates to this Policy

This Policy is the latest version as at 25/03/2024. The information set out in this Policy may change and the Policy may need to be revised. It is also appropriate to review the Policy and the information, processes, decisions and records documented in it from time to time.

This Policy will be reviewed at appropriate intervals by us to ensure that it remains up to-date and fit for purpose.

Who to contact about this Policy

For questions about this Policy, please contact Gurpreet Bassi the Secretary to the Trustees at pensionsmp@parliament.uk or call 0207 219 1356.

References

ICO guidance on Personal data breaches: Personal Data Breaches - ICO

Signed

Name Sir Brian H Donohoe

Chairman of the Trustees Date 25/03/2024

Appendix A: Personal data breach response plan