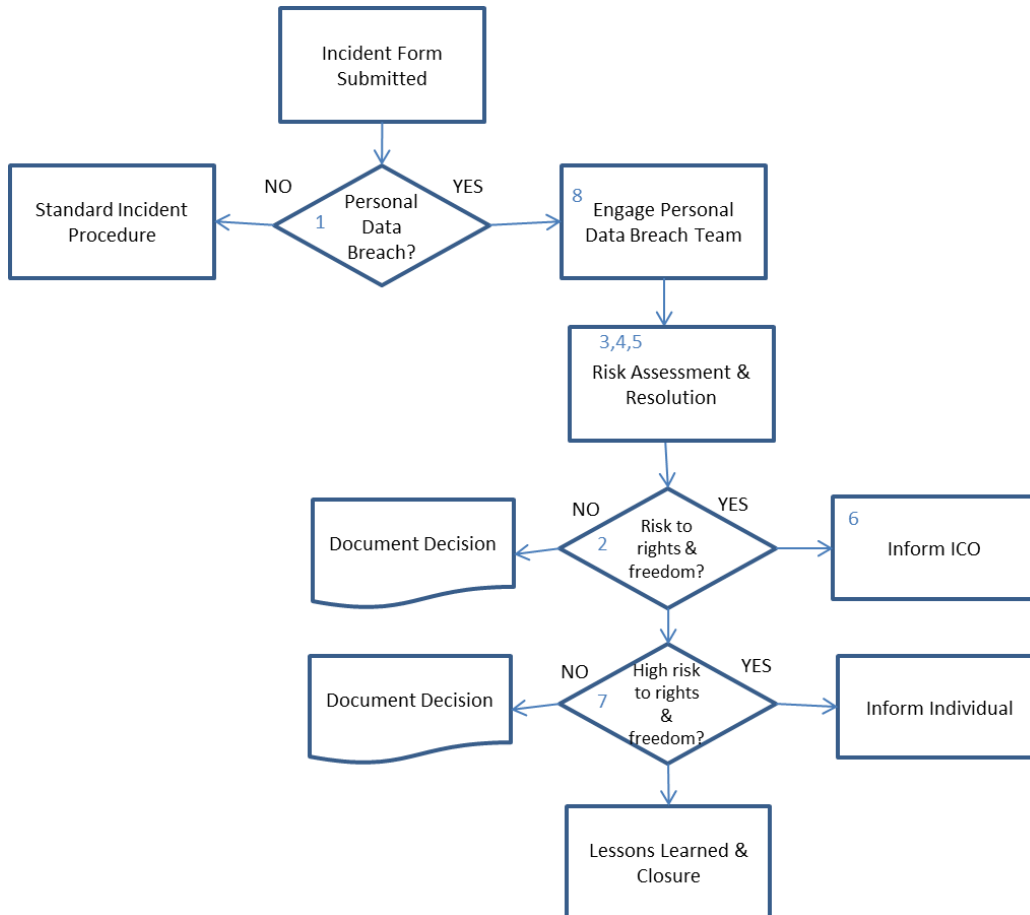


National Counties Building Society Pension and Life Assurance Scheme

Personal Data Breach Policy



1. What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (including 'personal sensitive 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.

Example

Personal data breaches can 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.

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, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Recital 87 of the GDPR makes clear that when a security incident takes place, we must quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

2. What breaches do we need to notify the ICO about?

When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we must notify the ICO; if it's unlikely then we don't have to report it. However, if we decide we don't need to report the breach, we need to be able to justify this decision, so it must be documented.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for scheme members. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on Scheme members, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect Scheme members whose personal data has been compromised. We need to assess this case by case, looking at all relevant factors.

Example

The theft of a Scheme member database, the data of which may be used to commit identity fraud, would need to be notified, given the impact this is likely to have on those Scheme members who could suffer financial loss or other consequences. On the other hand, we would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of an internal list.

So, on becoming aware of a breach, we should try to contain it and assess the potential adverse consequences for Scheme members, based on how serious or substantial these are, and how likely they are to happen.

3. How much time do we have to report a breach?

We must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If we take longer than this, we must give reasons for the delay.

Section II of the Article 29 Working Party Guidelines on personal data breach notification gives more details of when a controller can be considered to have “become aware” of a breach.

4. What information must a breach notification to the ICO contain?

When reporting a breach to the ICO, the GDPR says we must provide:

- a description of the nature of the personal data breach including, where possible:
 - the categories and approximate number of Scheme members concerned; and
 - the categories and approximate number of personal data records concerned;
- the name and contact details of the DPO or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

5. What if we don't have all the required information available yet?

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So Article 34(4) allows us to provide the required information in phases, as long as this is done without undue further delay.

However, the ICO expects controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. We must still notify the ICO of the breach when we become aware of it, and submit further information as soon as possible. If we know we won't be able to provide full details within 72 hours, we must explain the reason for the delay to the ICO and tell them when we expect to submit more information.

6. How do we notify a breach to the ICO?

For information about notifying the ICO of a personal data breach, refer to their website [pages on reporting a breach](#).

In the case of a breach affecting Scheme members in different EU countries, the ICO may not be the lead supervisory authority. This means that as part of our breach response plan, we should establish which European data protection agency would be our lead supervisory authority for the processing activities that have been subject to the breach. For more guidance on determining who the lead authority is, see the Article 29 Working Party [guidance on identifying your lead authority](#).

7. When do we need to tell Scheme members about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of Scheme members, the GDPR says we must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means the threshold for informing scheme members is higher than for notifying the ICO. Again, we will need to assess both the severity of the potential or actual impact on scheme members as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In

such cases, we will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing Scheme members is to help them take steps to protect themselves from the effects of a breach.

Notification to scheme members should as a minimum include:

- a description of how and when the breach occurred and what data was involved;
- the name and contact details of the DPO or other contact point;
- a description of the likely consequences of the breach; and
- details of the action taken or proposed to be taken to deal with the risks posed by the breach, including, where appropriate, measures to mitigate its possible adverse effects.

Clear and specific advice should be given as to how Scheme members can protect themselves and how they can get help. One of the factors to consider is whether Scheme members could act on the information provided to mitigate risks. In addition, CIFAS, the UK's Fraud Prevention Service suggests that scheme members who experience data loss should consider the following:

- Alert one of the three credit reference agencies (Experian, Equifax, Callcredit) who can help the scheme member review his credit report and identify any fraudulent entries. It will contact all of the organisations involved and also notify the other two credit reference agencies so they too can offer help. The credit report will be 'below the line' and scheme members can be assured that it will not have a negative impact on their credit score;
- Obtain CIFAS Protective Registration. For a small fee, a warning will alert most lenders to the fraud so that they can take extra care when dealing with credit applications in the scheme member's name.
- Inform the scheme member's bank, whether or not they are involved and it will monitor any bank accounts more closely.

It is important that affected Scheme members can contact the Trustees easily and gain information and help quickly. If a large number of Scheme members are affected, a dedicated telephone hotline and emergency email address will be set up to facilitate communication as appropriate.

Depending on the nature of the data loss and whether it occurred as a consequence of the Trustees' actions the Trustees should recompense Scheme members for any extra costs incurred in protecting themselves and consider compensation where appropriate.

Notification to the affected Scheme members is **not** required if any one of the three conditions below exists:

- (a) where we have implemented appropriate technical and organisational measures to protect personal data prior to the breach, in particular measures which render the data unintelligible to anyone not authorised to access it, for example by encryption;
- (b) where we have taken steps to ensure that the high risk posed to Scheme member's rights and freedoms is no longer likely to materialise. For example, the Trustees may have identified and

taken action against the person who unlawfully accessed the personal data before they were able to do anything with it; or

- (c) where it would involve disproportionate effort to contact the affected Scheme members, perhaps where their contact details are lost or were not known in the first place. In such circumstances, we must make a public communication or similar measure in respect of the breach.

8. Personal Data Breach Team – Incident Response Process

Incident Response Team – Core Members or their deputies are to be notified when a Personal Data breach has been reported Personal data breaches can also be notified to the team on an ad hoc basis outside of the Incident Reporting process.

Core Team Member	Name	Deputy
Trustee Representative	Chris Croft/Fiona Crisp/Mark Willis	
Society Representative	Vicki Webb	Patrizia Wakefield
Punter Southall Administrative Representative	Russell Porter	Troy Finch

Incident Response Team – Key Responsibilities

- I. **Risk Assessment** – Determine and document details of the incident and whether it is complete or ongoing.
- II. **Resolution** – Focus on recovery and containment
- III. **Escalation** – Who needs to be informed? e.g. ICO, scheme member, police, insurance, etc.
- IV. **Lessons Learned** – What can be learned from this incident and how do we improve our processes, systems and training to ensure the issue is not repeated.

V. 9. Do we notify anyone else?

- VI. On becoming aware of a serious personal data breach, the Pensions Regulator may need to be contacted. We must also consider whether any third parties should be notified, such as the police, insurers, bank or credit card companies who can assist in reducing the risk of financial loss to Scheme members.
- VII. We should also consider appointing an external representative to manage any communications with the public and media enquiries.

9. Frequency of Review

This policy will be reviewed on an annual basis by the Trustees to ensure its ongoing relevance and effectiveness.