



Personal Data Breaches Procedure

March 2023

Contents

Introduction2

Identifying a personal data breach2

Responsibilities3

Responding to an Information Security Incident.....3

Judging whether to report a breach to the ICO.....4

Reporting a breach to the ICO5

Communicating a breach.....6

Training6

Appendix I NESPF Breach Reporting Procedure7

Appendix II Breaches Register8

Appendix III Reporting Procedure Form9

Document	Personal Data Breaches Procedure
Review Date	March 2023
Approval Date	N/A
Author & Team	M Suttie, Governance
Review Date	March 2024

Introduction

This document has been prepared on behalf of Aberdeen City Council (as the 'administering authority') to assist the North East Scotland Pension Fund (the 'Fund') in identifying, responding to and reporting personal data breaches. Reporting of certain personal data breaches became mandatory under the General Data Protection Regulation (GDPR) from 25 May 2018. Following the United Kingdom's exit from the European Union, the EU GDPR has been kept in UK Law as the UK GDPR.

These procedure notes are supported by the NESPF Breaches of Law Policy as well as the ACC Corporate Information Handbook and Information Security Incident Reporting Procedure, available at <https://aberdeencitycouncil0365.sharepoint.com/SitePages/Policy,-Procedure,-Tools-and-Guidance.aspx>

Identifying 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.

Some examples are as follows:

- Access by an unauthorised third party (e.g. from failure to secure laptops, cabinets or leaving physical paperwork unattended)
- Deliberate or accidental action (or inaction) by a data controller or processor (e.g. password sharing, accessing personal data not required as part of your job, unsecure disposal, altering data without permission)
- Sending personal data to an incorrect recipient (e.g. due to human error or negligence)
- Computing devices containing personal data being lost or stolen (e.g. loss of a USB stick whether encrypted or non-encrypted)
- Loss of availability of personal data (e.g. due to software failure, operational disaster, encryption by ransomware)

Personal data defined under the UK GDPR is any information relating to an identified or identifiable natural person (the 'data subject'); and an identifiable natural person is one who can be identified, directly or indirectly by an identifier e.g. name, national insurance number etc.

Responsibilities

If an information security incident takes place, it must be quickly established whether a personal data breach has occurred and, if it has, steps promptly taken to address it.

In the case of a personal data breach, the data controller i.e. Aberdeen City Council as the administering authority of the Pension Fund, is required without undue delay and, where feasible, *not later than 72 hours after having become aware of it*, to notify the personal data breach to the supervisory authority, *unless* the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

In the United Kingdom, the independent supervisory body is the Information Commissioners Office (the 'ICO').

All NESPF staff have a responsibility for reporting information security incidents and near misses. An information security incident must be reported even if it appears to not have caused any harm. The main object of this procedure, rather than seek to apportion blame, is to close the breach and prevent or mitigate harm to those affected data subjects. Staff should be honest with the facts and assist with any investigation. Being thorough will allow valuable lessons to be learned with the aim of preventing future breaches.

Responding to an Information Security Incident

Officers must make their line manager aware of the incident and an initial report **must** be submitted **immediately** to the ICT Service Desk through [ServiceNow](#). This is the responsibility of the line manager, should they be absent another member of the management team should be informed and ensure the report is submitted.

The Governance Team must be copied into all communications regarding an information security incident.

Key steps to follow:

There are four key elements to any breach management plan, regardless of how the breach occurred:

1) [Containment and recovery](#)

On becoming aware of an incident, Officers need to take immediate action to contain the personal data breach e.g. finding a lost piece of equipment such as a USB stick or asking a recipient to return a document sent in error.

Following containment, it must be established whether there is anything further that can be done to recover any losses and limit the risk of damage from the breach e.g. using back up's to restore lost or damaged data.

2) Assessment of ongoing risk

An assessment should be carried out by those involved as to whether there are any ongoing risks resulting from the personal data breach. For example, consideration should be given to, what type of data is involved, its sensitivity, if any encryptions were in place, what harm could come from use of the data and any wider consequences.

3) Notification of breach

Judging whether a personal data breach needs to be reported and notified, to whom and in what timescale i.e. to the supervisory authority, the affected individuals etc. See following sections on 'Judging whether to report a breach' and 'Communicating a Breach'.

4) Evaluation and response

Evaluate effectiveness of response to the incident for example can any lessons be learnt, do policies or procedures need to be improved to address future incidents better, would staff benefit from further training on certain areas etc.

Judging whether to report a breach to the ICO

The relevant supervisory authority only needs to be notified where the breach is likely to result in a risk to the rights and freedoms of individuals; if unaddressed such a breach is likely to have a significant detrimental effect on individuals e.g. result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

The threshold to determine whether an incident needs to be reported to the ICO depends on the risk it poses to the people involved.

Not all personal data breaches need to be reported to the ICO.

Once the initial report is made to the ICT Service Desk, an initial assessment will be made to determine the severity of the incident, thereby determining what further course of action needs to follow. Each reported incident will be evaluated on a case by case basis.

No/low risk incidents will be managed within business as usual processes.

Medium/High Risk incidents will be escalated to the appropriate team(s) for incident response. Depending on the nature of the information security incident, the team involved in handling it will vary. However, each incident will have an Incident Handling Team Lead who will be responsible for coordinating the teams' efforts in containing, investigating and remedying the incident.

Reporting a breach to the ICO

In accordance with the UK GDPR certain information must be provided to the ICO when reporting a breach:

- Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- Communicate the name and contact details of the Data Protection Officer (the 'DPO') or other contact point where more information can be obtained;
- Describe the likely consequences of the personal data breach;
- Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

A notifiable breach must be reported to the relevant supervisory authority **within 72 hours** of the organisation becoming aware of it. However, it will often be impossible to investigate a breach fully in that short window and so the UK GDPR allows organisations to provide the information to the ICO in phases.

Where the notification to the ICO is made out with 72 hours, the notification must be accompanied by reasons for the delay.

Aberdeen City Council is required by virtue of section 5 of the Local Government and Housing Act 1989 to designate one of its officers as the 'Monitoring Officer' with a duty to report to the council on any proposal or decision that may be illegal, in breach of a code of practice, or likely to result in maladministration or injustice. In the event of a breach, Officers must also advise the Monitoring Officer (currently the Chief Officer-Governance).

Failing to report a personal data breach, when required to do so and within the regulatory timeframe, can have significant consequences for the administering authority (as the data controller for the NESPF) and/or individual staff members.

Therefore staff must ensure all information security incidents are reported through ServiceNow immediately to give sufficient time for ACC to assess the incident and determine whether they need to report to the ICO. If in doubt, please consult the Governance Team or the ACC DPO (dataprotectionofficer@aberdeencitycouncil.gov.uk) without delay.

Communicating a breach

Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller must communicate the personal data breach to the data subject without delay.

Any communication to the data subject shall describe in clear and plain language the nature of the personal data breach and must contain at least the information as set out in the previous section. The language should be open and direct, right to the point. Being transparent will allow the data subject to truly assess the risk to them and protect themselves.

However it should be noted that communication to the data subject will not be required where:

- The data controller has implemented appropriate technical and organisational protection measures and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- The data controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- It would be disproportionate effort. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

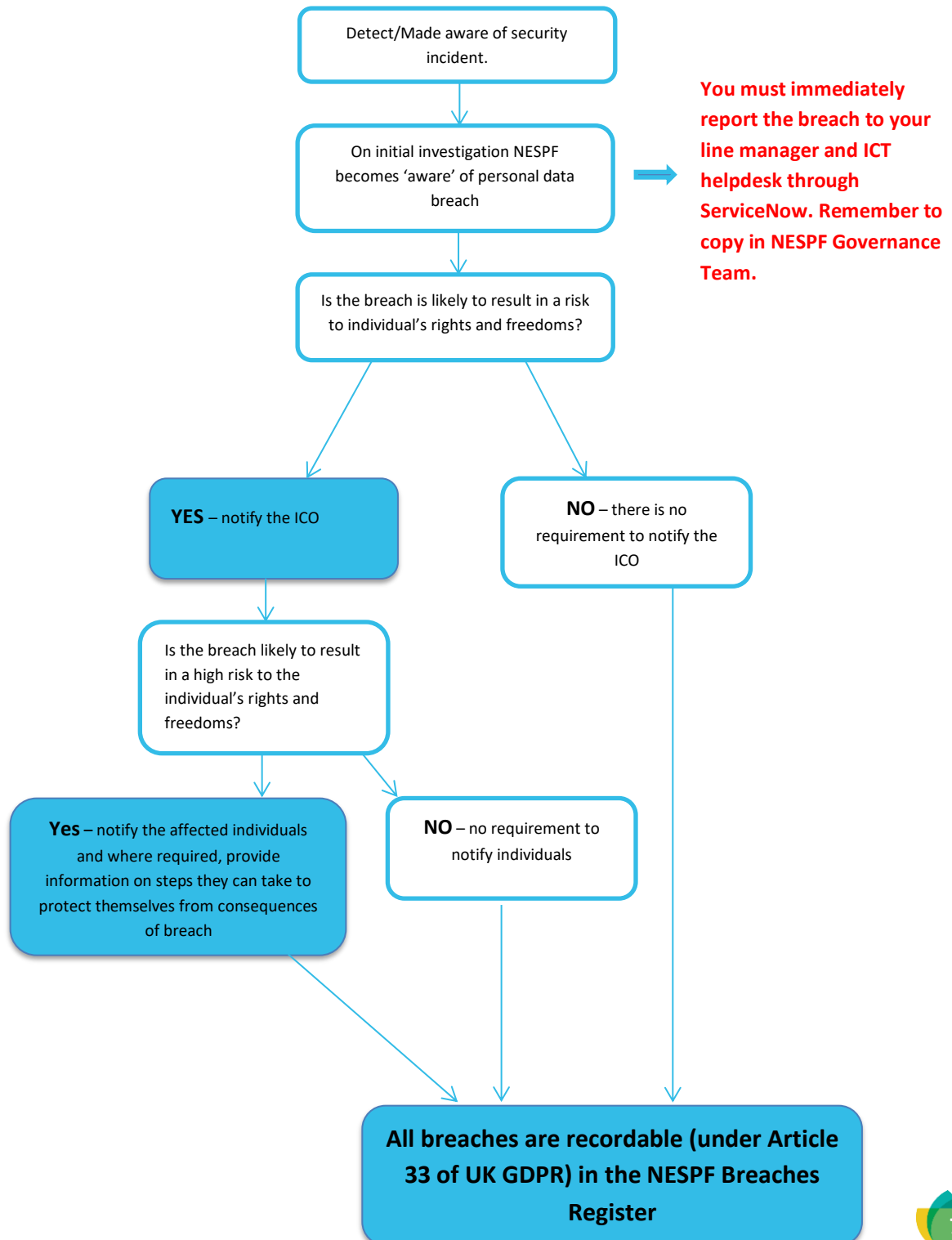
If the data controller has not already communicated the personal data breach to the data subject, the ICO, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to above are met.

Training

Internal training on breaches of law and data protection will be provided for Pension Fund staff, Pension Board and Pensions Committee members and stakeholders. Completion of the Information Governance online learning course through ACC Learn will be mandatory, and staff will be required to complete annual refresher training.

NESPF Breach Reporting Procedure

Appendix I




Example of Breaches Register

Appendix II

PENSION FUND BREACH REGISTER 2021/22								
No	Date of Breach	Category	Reported Data Breach on Service Now?	Brief Description	Potential Consequences of breach for individual(s)	Status/action to be undertaken to mitigate risk	Risk Matrix (consequences x likelihood of repeat)	Assess whether breach needs to be reported. If not, provide justification (see Breaches Policy for guidance)
1	11/10/2021	Contributions	Yes	Email was sent containing Scheme Member (30) personal data (Name, NiNo, Date of Birth, salary and contribution details) to the wrong recipient.	Potential harm to the individuals concerned who could be identified from the personal information or the information could be used for fraudulent means.	Unable to recall email. Staff to receive further training on data protection/secure email procedures.	<div> <div>Consequences</div> <div>Likelihood</div> </div>	Yes, the breach must be reported to ServiceNow and possibly to the ICO as it presents a risk to the rights and freedoms of affected individuals.
2	24/10/2021	Availability Breach	Yes	Personal data of member has been accidentally deleted from the administration system	Potential harm to the individual if the Pension Fund no longer has the information it needs to administer their benefits.	Ability to restore the data using system back ups. Review of system processes to be carried out.	<div> <div>Consequences</div> <div>Likelihood</div> </div>	Yes, the breach must be reported to ServiceNow. However it's unlikely the breach will need to be reported to the ICO as the incident only affected one individual, the information was only temporarily

Information Security Incident Reporting Procedure Form

To report an Information Incident or Data Protection Breach



For guidance on reporting an incident, see the [Information Security Incident Reporting Procedure](#).

Unsure if it's Personal Data - check [Appendix 1: Workflow: Is this personal data?](#)

If you need help filling in this form please refer to the [help sheet](#)

*** Reporting Officer**

▼

*** Cluster**

▼

Team

*** Third Tier Manager**

*** Type of Incident**

▼

*** Date & Time of Incident**

📅

*** Criticality Level**

▼

*** How was the incident discovered?**

⬆️⬆️

*** Incident Description (what and how)**

⬆️⬆️

*** What information was involved?**


⬆️⬆️

*** Was any hardware lost/damaged/compromised (laptop, mobile, usb drive, etc)?**

▼

*** Any Initial Actions Taken**

⬆️⬆️

 [Add attachments](#)