Data Breach Management Procedure

Date Reviewed: Sep 2021

Next Review: Sep 2024

Rosehill Housing Co-operative Limited
250 Peat Road, Pollok, Glasgow, G53 6SA
Tel: 0141 881 0595
Email: admin@rosehillhousing.co.uk
www.rosehillhousing.co.uk

DATA BREACH MANAGEMENT PROCEDURE

1 Introduction

1.1 This Procedure:

1.1.1 places obligations on staff to report actual or suspected personal data breaches; and

1.1.2 sets out our procedure for managing and recording actual or suspected personal data breaches.

1.2 This Procedure applies to all staff, and to all personal data and special category data held by us.

2 Definitions:

For the purposes of this Procedure:

Data Breach Team	means the members of staff at the organisation responsible for investigating personal data breaches;
data subject	means an individual to whom the personal data relates;
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 transmitted, stored or otherwise processed;
personal data	means information relating to an individual, who can be identified (directly or indirectly) from that information;
processing	means obtaining, recording, organising, storing, amending, retrieving, disclosing and / or destroying personal data, or using or doing anything with it; and
special category data	means personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an

individual) and information concerning an individual's health, sex life or sexual orientation.

3 Responsibility

The Data Protection Officer (DPO) has overall responsibility for this Procedure and for ensuring all staff comply with it.

4 Our duties

4.1 We process personal data about a number of categories of data subjects, including housing applicants, our tenants (and their household members), factored owners, job applicants, current and former employees, contractors, business contacts (including at other registered social landlords, regulators, local authorities and agencies), complainants, elected members, apprentices, committee members, and members for a number of specific lawful purposes relevant to our activities and functions as a registered social landlord in Scotland. As the controller of personal data, we have a responsibility under data protection legislation to protect the security of the personal data that we process about data subjects.

4.2 We must keep personal data secure against loss or misuse. All staff are required to comply with this Procedure.

5 What can cause a personal data breach?

A personal data breach can happen for several reasons:

5.1 loss or theft of equipment on which personal data is stored e.g. loss of a laptop or a paper file;

5.2 inappropriate access controls allowing unauthorised use of personal data;

5.3 equipment failure on which personal data is stored;

5.4 human error e.g. sending an e-mail containing personal data to the incorrect recipient;

5.5 unforeseen circumstances, such as damage to personal data due to a fire or flood;

5.6 hacking, phishing and other "blagging" attacks where personal data is obtained by deceiving whoever holds it;

5.7 alteration of personal data without permission; and

5.8 loss of availability of personal data.

6 If a personal data breach is discovered

6.1 If a member of staff knows or suspects that a personal data breach has occurred or may occur, they should contact the DPO immediately.

6.2 Staff should not take any further action in relation to the breach. Staff must not notify any affected data subjects or regulators. The DPO will take appropriate steps to deal with the breach in collaboration with the Data Breach Team.

7 Managing and recording the breach

7.1 On being notified of a suspected personal data breach, the DPO will notify the Data Breach Team, consisting of the DPO and the Finance Manager. The Data Breach Team will be led by the DPO.

7.2 The Data Breach Team will take immediate steps to establish whether a personal data breach has in fact occurred. If so, the Data Breach Team will take appropriate action to:

7.2.1 contain the data breach and (so far as reasonably practicable) recover, rectify or delete the personal data that has been lost, damaged or disclosed;

7.2.2 assess and record the breach in the Data Breach Risk Register;

7.2.3 notify appropriate parties (including the Information Commissioner's Office (ICO), Scottish Housing Regulator (SHR) and data subjects) of the breach; and

7.2.4 review the breach, its consequences and improvements that can be made.

These are explained in more detail below.

7.3 Containment and recovery

7.3.1 The Data Breach Team will within 24 hours of knowledge, where possible, identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data.

7.3.2 The Data Breach Team will identify ways to recover, correct or delete personal data. This may include contacting the Police e.g. where the breach involves stolen hardware or personal data.

7.3.3 Depending on the nature of the breach, the Data Breach Team will notify our insurer, as the insurer can provide access to data breach management experts, who may be able to assist us.

7.4 Assess and record the breach

7.4.1 Having dealt with containment and recovery within 48 hours of knowledge, the Data Breach Team will assess the risks associated with the breach, including:

(a) what type of personal data is involved?

(b) is the personal data, special category data?

(c) who is affected by the breach i.e. the categories and approximate number of data subjects involved?

(d) the likely consequences of the breach on affected data subjects e.g. what harm could come to those data subjects, are there risks to their physical safety, reputation, or financial loss?

(e) where personal data has been lost or stolen, are there any protections in place, such as encryption?

(f) what has happened to the personal data e.g. if personal data has been stolen, could it be used for harmful purposes?

(g) what could the personal data tell a third party about the data subject e.g. could the loss of apparently trivial snippets of personal data help a determined fraudster build up a detailed picture of the data subject and result in e.g. identity theft?

(h) what are the likely consequences of the personal data breach on our organisation e.g. loss of reputation or liability for fines?

(i) are there wider consequences to consider e.g. loss of public confidence in an important service that we provide?

7.4.2 Details of the breach will be recorded in the risk register by the Data Breach Team.

7.5 Notifying appropriate parties of the breach

7.5.1 The Data Breach Team will consider whether to notify:

(a) the ICO;

(b) affected data subjects;

(c) the Police; and

(d) other parties, including the SHR.

7.5.2 **Notifying the ICO**

(a) The Data Breach Team will notify the ICO when a personal data breach has occurred, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

(b) Where ICO notification is required, this shall be done without undue delay and, where feasible, not later than 72 hours after we became aware of it. Where the notification to the ICO is not made within 72 hours, it will be accompanied by reasons for the delay.

(c) If the Data Breach Team is unsure whether to report, the presumption should be to report. The Data Breach Team will take account of the factors set out below:

The potential harm to the rights and freedoms of data subjects	This is the overriding consideration in deciding whether a personal data breach should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. It can include: —exposure to identity theft through the release of non-public identifiers e.g. passport number; and —information about the private aspects of the data subject's life becoming known to others e.g. financial circumstances.
The volume of personal data	There should be a presumption to report to the ICO where: —a large volume of personal data is concerned; and —there is a real risk of data subjects suffering some harm. It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high e.g. because of the circumstances of the loss or the extent of

	information about each data subject.
The sensitivity of personal data	There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of data subjects suffering substantial detriment, including substantial distress. This is most likely to be the case where the breach involves special category data. In these circumstances, even a single record could trigger a report.

7.5.3 **Notifying data subjects**

(a) Where the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Breach Team will notify the affected data subjects without undue delay, including:

(i) the name and contact details of the DPO from whom more information can be obtained;

(ii) the likely consequences of the personal data breach; and

(iii) the measures we have or intend to take to address the personal data breach, including, where appropriate, recommendations for mitigating potential adverse effects.

(b) When determining whether and how to notify data subjects of the personal data breach, the Data Breach Team will:

(i) co-operate closely with the ICO and other relevant authorities e.g. the Police; and

(ii) take account of the factors set out in the table below:

Factor	Impact on obligation to notify data subject
Whether we have implemented and applied (to the affected personal data) appropriate technical and organisational protection measures — in particular, measures that render the personal data unintelligible to any person who is not authorised to access it by e.g. encryption.	Where such measures have been implemented, it is not necessary to notify the data subject.
Whether we have taken measures following the personal data breach which ensure the high risk to the rights and freedoms of data subjects affected by that breach is no longer likely to materialise.	Where such measures have been implemented, it is not necessary to notify the data subject.
Whether it would involve disproportionate effort to notify the data subject.	If so, it is not necessary to notify the data subject — but we must instead issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
Whether there are any legal or contractual requirements to notify the data subject?	If yes, it may be necessary to notify the data subject in any event.

7.5.4 **Notifying the Police**

The Data Breach Team will already have considered whether to contact the Police for the purpose of containment and recovery. Regardless of this, if it subsequently transpires that the breach arose from a criminal

act, the Data Breach Team will notify the Police and / or relevant law enforcement authorities.

7.5.5 **Notifying other parties**

The Data Breach Team will consider whether there are any legal or contractual requirements to notify any other parties, such as the SHR. We must report certain notifiable events to the SHR, including a serious breach of legislation. Depending on the circumstances, and subject to the advice of the DPO, a personal data breach may be regarded as a serious breach of data protection legislation and may therefore constitute a notifiable event to the SHR. The prior advice of the DPO must be obtained by staff in such circumstances.

7.6 Reviewing the breach and improvements

Once the personal data breach has been handled in accordance with this Procedure, the Data Breach Team will within one month of handling the personal data breach:

7.6.1 establish what security measures were in place when the breach occurred;

7.6.2 assess whether technical or organisational measures can be implemented to prevent the breach happening again;

7.6.3 consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or guidance;

7.6.4 consider whether it is necessary to conduct a new, or revisit an existing, data protection impact assessment of the personal data processing that was the subject of the breach;

7.6.5 update the risk register; and

7.6.6 debrief relevant Managers and other staff members following the investigation.

8 Staff awareness and training

8.1 Staff training and awareness raising is key to reducing the risks and occurrence of personal data breaches.

8.2 We provide regular data protection training to staff:

8.2.1 at induction;

8.2.2 when there is any change to the law, regulation or our policy;

8.2.3 when significant new threats are identified; and

8.2.4 in the event of a personal data breach occurring from which staff could learn.

9 Reporting breaches

Prevention is always better than cure. Data security concerns may arise at any time and we encourage staff to report any concerns to the DPO as soon as possible and at the earliest possible stage. This helps us capture risks as they emerge, protect us from personal data breaches, and keep our processes up-to-date and effective.

10 Consequences of failure to comply

10.1 Failure to comply with this Procedure puts us at risk. Failure to notify the DPO of an actual or suspected personal data breach is a very serious issue.

10.2 Staff may be liable to disciplinary action if they fail to comply with the provisions of this Procedure.

10.3 Due to the importance of this Procedure, failure to comply with any requirement of it may lead to disciplinary action for a member of staff under our procedures, and this action may result in dismissal for gross misconduct. If an external organisation breaches this Procedure, they may have their contract terminated by us with immediate effect.

10.4 Any questions or concerns about this Procedure should be directed to the DPO.

11 Review and updates to this Procedure

We will review and update this Procedure in accordance with our data protection obligations and we may amend, update or supplement it from time to time and at least every 3 years or earlier, if required by changes in legislation.