

ABBNEYFIELD SCOTLAND LIMITED

DATA BREACH MANAGEMENT POLICY

1 Introduction

1.1 This Policy:

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 Policy applies to all staff, and to all personal information and sensitive personal information held by us. This Policy supplements our Data Protection Policy and Information Security Policy.

1.3 We, Abbeyfield Scotland, will review and update this Policy in accordance with our data protection obligations and we may amend, update or supplement it from time to time.

1.4 Definitions:

For the purposes of this Policy:

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 information 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 information transmitted, stored or otherwise processed;

personal information 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 information, or using or

doing anything with it; and

sensitive personal information

means personal information 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.

2 Responsibility

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

3 Our duties

- 3.1 We process personal information relating to individuals, including our service users (and their next of kin), job and volunteer applicants, current and former employees and volunteers, contractors, suppliers, business contacts, consultants, Board members and donors. As the controller of personal information, we have a responsibility under data protection legislation to protect the security of the personal information that we hold about data subjects.
- 3.2 We must keep personal information secure against loss or misuse. All staff are required to comply with this Policy and our Data Protection Policy and Information Security Policy.

4 What can cause a personal data breach?

A personal data breach can happen for several reasons:

- 4.1 loss or theft of equipment on which personal information is stored e.g. loss of a laptop or a paper file;
- 4.2 inappropriate access controls allowing unauthorised use of personal information;
- 4.3 equipment failure on which personal information is stored;
- 4.4 human error e.g. sending an e-mail containing personal information to the incorrect recipient;
- 4.5 unforeseen circumstances, such as damage to personal information due to a fire or flood;
- 4.6 hacking, phishing and other "blagging" attacks where personal information is obtained by deceiving whoever holds it;

- 4.7 alteration of personal information without permission; and
- 4.8 loss of availability of personal information.

5 If a personal data breach is discovered

- 5.1 If a member of staff knows or suspects that a personal data breach has occurred or may occur, they should contact the DPO immediately.
- 5.2 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.

6 Managing and recording the breach

- 6.1 On being notified of a suspected personal data breach, the DPO will notify the Data Breach Team, consisting of the DPO, [INSERT DETAILS OF OTHER STAFF MEMBERS]. The Data Breach Team will be led by the DPO.
- 6.2 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:
 - 6.2.1 contain the data breach and (so far as reasonably practicable) recover, rectify or delete the personal information that has been lost, damaged or disclosed;
 - 6.2.2 assess and record the breach in the data breach register;
 - 6.2.3 notify appropriate parties (including the Information Commissioner's Office (ICO), Scottish Housing Regulator (SHR) and data subjects) of the breach; and
 - 6.2.4 take steps to prevent future breaches.

These are explained in more detail below.

6.3 Containment and recovery

- 6.3.1 The Data Breach Team will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal information.
- 6.3.2 The Data Breach Team will identify ways to recover, correct or delete personal information. This may include contacting the Police e.g. where the breach involves stolen hardware or personal information.
- 6.3.3 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.

6.4 Assess and record the breach

6.4.1 Having dealt with containment and recovery, the Data Breach Team will assess the risks associated with the breach, including:

- (a) what type of personal information is involved?
- (b) is the personal information, sensitive personal information?
- (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 information has been lost or stolen, are there any protections in place, such as encryption?
- (f) what has happened to the personal information e.g. if personal information has been stolen, could it be used for harmful purposes?
- (g) what could the personal information tell a third party about the data subject e.g. could the loss of apparently trivial snippets of personal information 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?

6.4.2 Details of the breach will be recorded in the data breach register by the Data Breach Team.

6.5 Notifying appropriate parties of the breach

6.5.1 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.

6.5.2 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:

<p>The potential harm to the rights and freedoms of data subjects</p>	<p>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:</p> <ul style="list-style-type: none"> —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.
<p>The volume of personal information</p>	<p>There should be a presumption to report to the ICO where:</p> <ul style="list-style-type: none"> —a large volume of personal information is concerned; and —there is a real risk of data subjects suffering some harm. <p>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</p>

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

6.5.3 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	Where such measures have been implemented, it

Factor	Impact on obligation to notify data subject
(to the affected personal information) appropriate technical and organisational protection measures — in particular, measures that render the personal information unintelligible to any person who is not authorised to access it by e.g. encryption.	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.

6.5.4 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.

6.5.5 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.

6.6 Preventing future breaches

Once the personal data breach has been handled in accordance with this Policy, the Data Beach Team will:

- 6.6.1 establish what security measures were in place when the breach occurred;
- 6.6.2 assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- 6.6.3 consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or guidance;
- 6.6.4 consider whether it is necessary to conduct a new, or revisit an existing, data protection impact assessment of the personal information processing that was the subject of the breach;
- 6.6.5 update the data breach register; and
- 6.6.6 debrief Data Breach Team members following the investigation.

7 Staff awareness and training

- 7.1 Staff training and awareness raising is key to reducing the risks and occurrence of personal data breaches.
- 7.2 We provide regular data protection training to staff:
 - 7.2.1 at induction;
 - 7.2.2 when there is any change to the law, regulation or our policy;
 - 7.2.3 when significant new threats are identified; and
 - 7.2.4 in the event of a personal data breach occurring from which staff could learn.

8 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.

9 Consequences of failure to comply

- 9.1 Failure to comply with this Policy puts us at risk. Failure to notify the DPO of an actual or suspected personal data breach is a very serious issue.
- 9.2 Staff may be liable to disciplinary action if they fail to comply with the provisions of this Policy.
- 9.3 Due to the importance of this Policy, 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 Policy, they may have their contract terminated by us with immediate effect.
- 9.4 Any questions or concerns about this Policy should be directed to the DPO.

Last updated: August 2018