# PERSONAL DATA BREACH POLICY

## 1. POLICY STATEMENT

1.1 This policy is to be read in conjunction with our policies on data protection and any other related policies or documents, including any data protection Privacy Notices supplied to individuals we deal with.

1.2 We have a commitment to ensuring that Personal Data, as defined in our policies on data protection, is processed in line with UK GDPR and relevant UK law and that all members of staff conduct themselves in line with this and other related policies. We have strict obligations to process Personal Data securely, adopt sufficient procedural and technological safeguards and lawfully handle data breaches. Our obligations include, in the event of a data breach, notifying the relevant authorities and, in some cases, affected individuals.

1.3 The purpose of this policy is to explain what is required from you if you discover that Personal Data may have been lost, used or disclosed in an unauthorised way, amounting to a personal data breach, and our stance on taking action in line with data protection obligations if a breach were to occur.

1.4 If you consider that this policy has not been followed in any respect, you should raise the matter with the Privacy Officer, your manager, or a Director.

1.5 This policy does not form part of any employee's contract of employment and it may be amended at any time. We may also vary this policy, including any time limits, as appropriate in any case.

1.6 Any breach of this policy will be taken seriously and may result in disciplinary action.

## 2. WHO IS COVERED BY THIS POLICY?

2.1 This policy applies to all employees, directors and other officers, workers and agency workers, volunteers and interns.

2.2 We also require in any contracts with third parties who may have access to any Personal Data, such as consultants, contractors or suppliers, that they comply with this policy. We will ensure they are given access to a copy.

2.3 All individuals covered in sections 2.1 and 2.2 are referred to as 'staff' in this policy.

## 3. WHO IS RESPONSIBLE FOR THIS POLICY?

3.1 Our Privacy Officer is responsible for ensuring compliance with UK GDPR and with this policy. your manager can advise you who our Privacy Officer is. If we have cause to appoint a Data Protection Officer (an official appointment) or use a different title for a Privacy Officer, we will let you know and any reference to Privacy Officer shall include reference to a new title or a Data Protection Officer. Any questions or concerns about the operation of this policy should be referred in the first instance to the Privacy Officer.

3.2 While we ask all managers to work with the Privacy Officer to make sure this policy is complied with, its successful operation also depends on you. Please take the time to read and understand it and to go back to the Privacy Officer or your manager with any questions you may have. References to Directors in this policy mean the most senior people within our organisation.

## 4. WHAT IS A PERSONAL DATA BREACH?

4.1 A personal data breach is a security incident that has affected the confidentiality, integrity or availability of Personal Data.

4.2 A personal data breach is wider in scope than just the loss of Personal Data. The following are examples of personal data breaches:

a) access by an unauthorised third party,

b) deliberate or accidental action (or inaction),

c) sending Personal Data to an incorrect recipient,

d) computing devices containing Personal Data being lost or stolen,

e) alteration of Personal Data without permission, and/or

f) loss of availability of Personal Data.

## 5. YOUR RESPONSIBLITIES

5.1 It is our aim to secure and protect Personal Data and not to have cause to use this personal data breach notification policy. While we can put measures in place, we also require you to comply with all of those security measures and to understand and follow all our other policies on data protection.

5.2 You are also required to be vigilant and look out for potential data security issues, such as:

a) someone is printing off a large amount of Personal Data,

b) someone is taking Personal Data out of the office and there is no obvious reason for this,

c) someone has emailed Personal Data to their personal email address,

d) you receive requests for Personal Data from third parties or even

other staff members but there is no explanation, or the explanation given is questionable,

e) you become aware that emails from your account have been sent without your authority,

f) you become aware that your computer or device is being controlled by a third party,

g) you receive a call or email from someone unknown and unauthorised, claiming to manage your IT system, asking you to click links, give your login details or have access to your computer,

h) you receive a call or email from someone unknown and unauthorised, claiming to be from a reputable company (for example, Microsoft, Virus protectors, IT companies) asking you to confirm subscriptions or allow them to access your computer, or

i) you receive any calls or emails that are unexpected and/or raise suspicion.

5.3 We require you to inform the Privacy Officer and your manager immediately if you:

a) become aware that any of our policies on data protection are not being followed,

b) become aware of a personal data breach (even if you are in part or in full responsible for the breach),

c) suspect a personal data breach, may have happened, or

d) become aware of, or suspect there is, a risk of a personal data breach, whether involving our activities or those of other Staff, or a third-party processor.

5.4 You are not permitted to disclose details of a potential personal security issue to any third party unless you have been given permission to do so. We have strict obligations to report data security breaches in accordance with the law, and disclosing it without our control will not allow us to do this. In particular, you are not permitted to discuss data security or breaches with the press. If in doubt, please speak to the Privacy Officer, your manager or a Director, and/or refer to our Whistleblowing Policy.

5.5 If you feel you require training or guidance on any of our policies or any instructions we give you, it is your responsibility to speak to the Privacy Officer or your manager.

## 6. ASSESSING THE BREACH

6.1 In the event that a breach is identified, the Privacy Officer will:

a) enter details of the breach into our personal data breach records,

b) carry out an investigation into what happened and take appropriate steps to restrict the consequences of the breach,

c) assess whether the breach needs to be reported to the Information Commissioner's Office (ICO),

d) assess whether the affected individual needs to be informed of the breach, and

e) assess whether any third parties or other authorities need to be informed.

## 7. NOTIFIABLE BREACHES

7.1 A personal data breach will be a notifiable breach if it is likely to pose a risk to an individual's rights and freedoms.

7.2 A risk to people's freedoms can include physical, material or non-material damage, such as discrimination, identity theft or fraud, financial loss and damage to reputation.

7.3 In some cases, the breach will easily be identified as notifiable, for example, a list of individual customers, their addresses and their bank details has been stolen by an ex-employee. In other cases, it will be necessary to assess the likelihood of the risks to an individual's rights and freedoms.

7.4 When making an assessment of the risks, the following will need to be considered and recorded:

a) type of breach,

b) nature, sensitivity and volume of Personal Data,

c) ease of identification of individuals,

d) severity of consequences for individuals,

e) any special characteristics of the individual (for example, children or other vulnerable individuals may be at greater risk),

f) number of individuals affected, and

g) specific characteristics of the Data Controller (for example, a medical organisation processing sensitive personal information such as Special Category Data will pose a greater threat than the mailing list of a newspaper).

## 8. NOTIFICATION TO THE ICO

8.1 It is our responsibility as Data Controller to notify the ICO of the notifiable breaches.

8.2 The Privacy Officer is responsible for notifying and dealing with the ICO.

8.3 Notifications must be made without undue delay and no later than 72 hours after becoming aware of the breach. If it is not possible to notify the ICO within the required 72 hours, we will provide an explanation within 72 hours.

8.4 The following information will be provided when a breach is notified:

a) a description of the nature of the personal data breach, including, where possible, the categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned,

b) the name and contact details of the Privacy Officer or a Director to approach for further information,

c) a description of the likely consequences of the personal data breach, and

d) 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.

8.5 If it has not been possible to conduct a full investigation into the breach and it is not possible to give all the required details within 72 hours, we will provide the ICO with the information we have, give reasons for the incomplete notification and an estimated timetable for full notification. The initial notification will be followed up with further details.

## 9. NOTIFICATION TO AFFECTED INDIVIDUALS

9.1 Where a notifiable breach has a high risk to the rights and freedoms of individuals, we have a duty to notify the affected individuals. High risk may be, for example, where there is an immediate threat of identity theft, or if Special Category Data is disclosed online.

9.2 It is our responsibility as Data Controller to notify the individuals of the notifiable breach.

9.3 The Privacy Officer or a Director is responsible for notifying and dealing with the affected individuals.

9.4 Notifications of notifiable personal data breaches to affected individuals must be made without undue delay and may be made before notifying the ICO if necessary.

9.5 The following information will be provided when a breach is notified:

a) a description of the nature of the personal data breach,

b) the name and contact details of the Privacy Officer or a Director to approach for further information,

c) a description of the likely consequences of the personal data breach, and

d) 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.

## 10. RECORD OF BREACHES

10.1 We will record all personal data breaches, regardless of the severity of the risk involved and whether they are notifiable or not. Our records will include the nature of the personal data breach, the consequences and the remedial action taken.

10.2 We will review any personal data breaches on a regular basis, learn from them and take appropriate steps to minimise any future risks.

## 11. MONITORING AND REVIEW OF THE POLICY

11.1 We will continue to review the effectiveness of this policy to ensure it

is achieving its stated objectives.