Persona data policy

Version 1	September 2018
Agreed by SMT	
Review date	September 2020

1. Scope

This procedure applies in the following events:

1. A personal data breach pursuant to Article 33 '*Notification of a personal data breach to the supervisory authority',* and

2. A personal data breach pursuant to Article 34 *'Communication of a personal data breach to the data subject'* of the GDPR.

2. Data controller and data processor

There is a distinction under the GDPR between a 'data controller' and a 'data processor'. This is because different organisations involved in processing personal data have varying degrees of responsibility. An organisation must choose whether it is a data controller or a data processor.

3. Responsibility

All users, including temporary employees of Age UK East London and third parties, and Age UK East London must be aware of this procedure and are required to follow it should a personal data breach incident occur.

4. Procedure – Breach Notification

Data processor to data controller

All personal data breaches by Age UK East London must be notified to the appropriate data controller immediately. The Data Protection Officer ("DPO") must record the communication of the breach in the Data Breach Register, stating how the notification was made (whether by email, telephone call etc.), to whom and how the confirmation of receipt was provided.

Data controller to supervisory authority

If a risk is considered likely, Age UK East London is required to report the personal data breach to the supervisory authority immediately and in any event, no later than 72 hours after they have been aware about the breach. If the notification is made outside of the 72 hour window, Age UK East London is required to provide reasons for the delay.

Age UK East London is required to provide the following to the supervisory authority:

- A description of the nature of the personal data breach;
- The categories of personal data that have been affected by the breach;

- The number, which may be approximated if necessary, of data subjects affected by the breach;
- The number, which may be approximated if necessary, of personal data records affected by the breach;
- The name and contact details of the DPO;
- The likely outcomes of the personal data breach;
- Any measures taken by Age UK East London to address and/or mitigate the breach; and
- All other information regarding the data breach.

The DPO must record the communication of the breach in the Data Breach Register, stating how the notification was made (whether my email, telephone call etc.), to whom and how the confirmation of receipt was provided.

Data controller to data subject

If it is likely that there will be a high risk to the affected data subject's rights and freedoms under the GDPR, Age UK East London is required to provide immediate notification to the relevant data subjects.

The notification to the data subject must be made in clear and plain language and must include the following:

- A description of the nature of the personal data breach;
- The categories of personal data that have been affected by the breach;
- The number, which may be approximated if necessary, of data subjects affected by the breach;
- The number, which may be approximated if necessary, of personal data records affected by the breach;
- The name and contact details of the DPO;
- The likely outcomes of the personal data breach;
- Any measures taken by Age UK East London to address and/or mitigate the breach; and
- All other information regarding the data breach.

Age UK East London must use appropriate measures, such as encryption, to ensure that all personal data is secure and cannot be accessed by those without the requisite authority.

Age UK East London must also take subsequent measures to ensure that the risk to the rights and freedoms of the data subject are no longer an issue.

If notification would require Age UK East London to implement a disproportionate amount of effort, a public communication or other similar measure may suffice, so long as all data subject are effectively informed.

It is possible that the supervisory authority may require Age UK East London to communicate the personal data breach to the data subject, should there be an element of high risk involved.