Age UK East London
Security Incident & Data Breach Policy & Procedure
Version 2.1

---

1. Introduction

1.1 This Policy sets out the obligations of Age UK East London a company registered in England under number 07687015, whose registered office is at 2nd Floor, 82 Russia Lane, Bethnal Green, London E2 9LU ("the Company") regarding the handling and reporting of security incidents and data breaches in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

1.2 The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

1.3 The GDPR defines a "personal data breach" as 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.

1.4 The Company is under a duty to report certain types of personal data breach directly to the UK's supervisory authority, the Information Commissioner's Office ("ICO"). The Company is also required to inform individual data subjects in the case of breaches that present a high risk of adversely affecting their rights and freedoms.

1.5 All personal data collected, held, and processed by the Company will be handled in accordance with the Company's Data Protection Policy.

1.6 The Company has in place procedures for the detection, investigation, and reporting of security incidents and data breaches. This Policy applies to all security incidents and data breaches (including personal data breaches) within the Company and is designed to assist in both the handling of such incidents and breaches and in determining whether or not they must be reported to the ICO and/or to data subjects.

1.7 The Company's Senior Information Risk Officer (SIRO) in conjunction with the Company's Data Protection Officer (DPO) is responsible for the implementation of this Policy, for overseeing the handling of all data breaches, and for ensuring that this Policy is adhered to by all staff.

2. Scope of Policy

2.1 This Policy relates to all information systems employed by the Company and all formats of data (including personal data and sensitive personal data (known

as "special category" under the GDPR)) collected, held, and processed by the Company.

2.2 This Policy applies to all staff of the Company, including but not limited to employees, agents, contractors, consultants, temporary staff, volunteers, casual or agency staff, or other suppliers or data processors working for or on behalf of the Company.

2.3 This Policy applies to all security incidents and data breaches, whether suspected or confirmed.

3. Security Incidents and Data Breaches

3.1 For the purposes of this Policy, a security incident or data breach means any event or action (accidental or deliberate) which presents a threat to the security, integrity, confidentiality, or availability of any Company information system or data.

3.2 Incidents to which this Policy applies may include, but not be limited to:

a) the loss or theft of a physical data record or records;

b) the loss or theft of computer equipment (e.g. laptop), mobile devices (e.g. smartphone or tablet), portable data storage devices (e.g. USB drive), or other data storage devices;

c) damage to equipment, whether deliberate or accidental;

d) equipment failure;

e) unauthorised access to, use of, or modification of data (or inadequate access controls allowing unauthorised access, use, or modification);

f) unauthorised disclosure of data;

g) human error (e.g. sending data to the wrong recipient);

h) unforeseen circumstances such as fire or flood;

i) hacking, phishing, and other 'blagging" offences whereby information is obtained by deception;

4. Internal Reporting

4.1 If a security incident or data breach is discovered or suspected, the individual or individuals discovering it should immediately make a report to IT support (e.g. via the IT Helpdesk).

4.2 It is also the duty of the individual or individuals discovering the security incident or data breach to report the matter to the Company's SIRO.

4.3 To ensure that the SIRO has been informed, the IT Helpdesk must also report the matter to the SIRO.

4.4 The SIRO is responsible for ensuring that a Security Incident or Data Breach Report Form, is completed. A template is appended to this Policy.

4.5 The completed Security Incident or Data Breach Report Form should include full and accurate details about the incident including, but not limited to (where applicable):

a) the time and date of the breach;

b) the time and date the breach was discovered;

c) equipment or systems involved;

d) people involved;

e) the type(s) of data involved;

f) where the breach involves personal data, the categories(s) of data subject to which the personal data relates (e.g. customers, employees etc.);

g) whether or not any sensitive personal data is involved;

h) how many data subjects are likely to be affected (if known);

4.6 Where appropriate, members of staff should liaise with their line managers when completing or assisting in the completion of Security Incident or Data Breach Report Forms.

4.7 If a data breach occurs or is discovered outside of normal working hours, it should be reported as soon as is reasonably practicable.

4.8 Unless and until instructed to by the SIRO or DPO, individuals should not take any further action with respect to a security incident or data breach. In particular, individuals should not take it upon themselves to notify affected data subjects, the ICO, or any other individuals or organisations.

5. Initial Management and Recording

5.1 Upon receipt of a Security Incident or Data Breach Report Form (or upon being notified of a security incident or data breach in any other way), the Company's SIRO shall begin by determining whether the data breach is still occurring. If this is the case, appropriate steps shall be taken immediately to minimise the effects of the data breach and to stop it.

5.2 Having established the above, the following steps shall then be taken with respect to the data breach:

a) undertake an initial assessment of the data breach, liaising with the relevant staff, IT Support and departments where appropriate.

b) establish the severity of the data breach and decide whether to assemble an Incident Response Team.

c) contain the data breach and, to the extent reasonably practicable, recover, amend, or restrict the availability of (e.g. by changing or revoking access permissions or by temporarily making the data unavailable electronically) the affected data;

d) determine whether anything further can be done to recover the data and/or other losses, and to limit the damage caused by the breach;

e) establish who needs to be notified initially (including, if physical records or equipment have been lost or stolen, the police) as part of the initial containment;

f) determine, in liaison with the relevant staff, departments and suppliers, the best course of action to resolve and remedy the data breach; and

g) record the breach and the initial steps taken above in the Company's Data Breach Register.

5.3 After the initial steps described above and when the threats posed by the incident have been removed, the Company's Data Protection Officer (DPO) will initiate an investigation and assessment of the incident or data breach as described in Section 6, below.

6. Investigation and Assessment

6.1 The Company's Data Protection Officer will instigate an investigation of a security incident or data breach as soon as is reasonably possible after receiving a copy of the Data Breach Report Form (or being notified in any other way) and, in any event, within 24 hours of the data breach being discovered and/or reported.

6.2 Investigations and assessments must take the following into account:

a) the type(s) of data involved (and, in particular, whether the data is personal data or sensitive personal data);

b) the sensitivity of the data (both commercially and personally);

c) what the incident or data breach involved;

d) what organisational and technical measures were in place to protect the data;

e) what might be done with the data as a result of an incident or breach (including unlawful or otherwise inappropriate misuse);

f) where personal data is involved, what that personal data could tell a third party about the data subjects to whom the data relates;

g) the category or categories of data subject to whom any personal data relates;

h) the number of data subjects (or approximate number if calculating an exact number is not reasonably practicable) likely to be affected by the data breach;

i) the potential effects on the data subjects involved;

j) the potential consequences for the Company;

k) the broader consequences of the incident or data breach, both for data subjects and for the Company;

6.3 The results of the investigation and assessment described above must be recorded in the Company's Security Incident and Data Breach Register.

6.4 Having completed the investigation and assessment described above, the DPO willl determine the parties to be notified of the breach as described below.

7. Notification

7.1 The Company's Data Protection Officer will determine whether to notify one or more of the following parties of the incident or breach:

a) affected data subjects;

b) the Information Commissioner's Office (ICO);

c) the police;

d) the Company's insurers;

e) The Company's legal advisors;

f) affected commercial partners;

7.2 When considering whether (and how) to notify individual data subjects in the event of a personal data breach, the following should be considered:

a) the likelihood that data subjects' rights and freedoms as set out in the GDPR (and the Company's Data Protection Policy) will be adversely affected;

b) whether there is a legal or contractual requirement to notify;

c) whether measures in place to protect the affected personal data (e.g. pseudonymisation or encryption) have been applied, thereby rendering the data unusable to any unauthorised parties;

d) whether measures have been taken following the data breach that will ensure that a high risk to the rights and freedoms of affected data subjects is no longer likely to occur;

e) the benefits to data subjects' of being notified (e.g. giving them the opportunity to mitigate the risks posed by the data breach);

f) whether notifying individuals will involve disproportionate effort (in which case a public communication or other widely available notice may suffice, provided that affected data subjects will still be informed effectively);

g) the best way of notifying data subjects, taking into account the urgency of the situation and the security of the possible methods;

h) any special considerations applicable to certain categories of data subject (e.g. children or vulnerable people);

i) the information that should be provided to affected data subjects;

j) how to make it easy for affected data subjects to contact the Company to find out more about the data breach;

k) further assistance that the Company should provide to the affected data subjects, where appropriate;

l) the risks of over-notifying – not all data breaches require notification and excessive notification may result in disproportionate work and numbers of enquiries from individuals;

7.3 When individual data subjects are to be informed of a personal data breach, those individuals must be informed of the breach without undue delay. Individuals shall be provided with the following information:

a) a user-friendly description of the data breach, including how and when it occurred, the personal data involved, and the likely consequences;

b) clear and specific advice, where relevant, on the steps individuals can take to protect themselves;

c) a description of the measures taken (or proposed to be taken) to address the data breach including, where relevant, measures taken to mitigate any possible adverse effects;

d) contact details for the Company's Data Protection Officer from whom affected individuals can obtain further information about the data breach.

7.4 When considering whether (and how) to notify the ICO of a data breach, the following should be considered:

a) the risk and potential harm to data subjects, their rights, and freedoms – harm can include (but is not limited to) financial harm, physical harm, loss of control over personal data, discrimination, identity theft or fraud, damage to reputation, and emotional distress;

b) the volume of personal data involved – the ICO should be notified if a large volume of data is involved and there is a real risk of data subjects suffering harm as a result, however it may also be appropriate to notify the ICO if a smaller amount of high-risk data is involved;

c) the sensitivity of the data involved – the more sensitive the personal data is, the less the volume of it is relevant and if the data breach presents a significant risk of data subjects suffering substantial detriment or distress, the ICO should be notified.

7.5 If the ICO is to be notified of a data breach, this must be done within 72 hours of becoming aware of the breach, where feasible. This time limit applies even if complete details of the data breach are not yet available. The ICO must be provided with the following information:

a) the category or categories and the approximate number of data subject whose personal data is affected by the data breach;

b) the category or categories and the approximate number of personal data records involved;

c) the name and contact details of the Company's Data Protection Officer from which the ICO can obtain further information about the data breach;

d) a description of the likely consequences of the data breach; and

e) a description of the measures taken (or proposed to be taken) to address the data breach including, where relevant, measures taken to mitigate any possible adverse effects.

7.6 The police may have been contacted at an earlier point in the data breach procedure (see 5.2), however further investigation may reveal that the data breach resulted from a criminal act, in which case the police should be further informed.

7.7 Records must be kept of all data breaches, regardless of whether notification is required. The decision-making process surrounding notification should be documented and recorded in the Company's Data Breach Register.

8. Evaluation and Response

8.1 When the steps set out above have been completed, the incident or data breach has been contained, and all necessary parties notified, the Company's Data Protection Officer shall conduct a complete review of the causes of the data breach, the effectiveness of the measures taken in response, and whether any systems, policies, or procedures can be changed to prevent data breaches from occurring in the future.

8.2 Such reviews shall, in particular, consider the following with respect to data (and in particular, personal data) collected, held, and processed by the Company:

a) where and how data is held and stored;

b) the current organisational and technical security measures in place to protect data and the risks and possible weaknesses of those measures;

c) the methods of data transmission for both physical and electronic data and whether or not such methods are secure;

d) the level of data sharing that takes place and whether or not that level is necessary;

e) whether any data protection impact assessments need to be conducted or updated;

f) staff awareness and training concerning data protection;

8.3 Where possible improvements and/or other changes are identified, the Company's Data Protection Officer shall liaise with the Senior Information Risk Officer (SIRO) and relevant staff with respect to the implementation of such improvements and/or changes.

9. Review and Implementation

9.1 This Policy and Procedure, together with the attached Form shall be deemed effective as of 18th March 2020. No part of this Policy and Procedure shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

9.2 This Policy, Procedure and Form will be updated as necessary to reflect current best practice, official guidance, and in line with current legislation.

9.3 This Policy, Procedure and Form will be reviewed at least annually.

9.4 The latest version of this Policy, Procedure and Form document will be made readily available to all employees, agents, contractors, volunteers or other parties working on behalf of the Company.

This Policy, Procedure and Form have been approved and authorised by:

Name:	Jane Caldwell
Position:	Chief Executive
Date:	18th March 2020
Due for Review by:	17th March 2021
Signature:	

10. Change history

Version	Section	Issue	Change	Approval	Date
1.0	n/a	Original document	n/a	CEO	05/06/2018
2.0	n/a	Not fully GDPR compliant	Complete rewrite	DPO	04/03/2020
2.0	5.2	Review	Specified at least annual reviews in line with DS&P Toolkit	DPO	04/03/2020
2.1	0	Title	Added Security Incident to title to reflect procedure content	DPO	14/03/2020
2.1	All	Scope restricted	Revised all content to include the wider scope of all security incidents	DPO	14/03/2020
2.1	Appendix	Example Report Form needed	Added Security Incident or Data Breach Report Form as Appendix	DPO	14/03/2020

Age UK East London
Security Incident or Data Breach Report Form
Version 2.1

No.	Item	Report response
1	**INCIDENT NUMBER** (TO BE COMPLETED BY SIRO/DPO)	**INCIDENT TITLE** (TO BE COMPLETED BY SIRO/DPO)
2	Person reporting the incident/breach *Give name and contact details*	
3	Who was the incident reported to? *Give name(s) and where relevant, call log numbers etc.*	
	Was the incident reported to the Police? *If so, record the Crime Number*	
4	Date and time of the incident (if known). *State if actual or estimated*	
5	Date and time the incident or breach was discovered.	
6	Place that the incident occurred.	
7	Equipment and/or systems involved.	

Age UK East London
Security Incident or Data Breach Report Form
Version 2.1

No.	Item	Report response
8	People and organisations involved *Include names where known and roles e.g. witness, data subject, suspect etc.*	
9	Type(s) of data involved.	
10	Where the breach involved personal data, specify the categories(s) of data subject to which the personal data relates *e.g. clients, employees etc.*	
11	Specify any sensitive personal data involved.	
12	Estimated number of data subjects are likely to be affected.	

Age UK East London
Security Incident or Data Breach Report Form
Version 2.1

No.	Item	Report response
13	Description of the security incident or data breach. *Continue on a separate sheet if necessary*	