

PROCESSING BY EXTERNAL SUPPLIERS POLICY

Version 4	June 2022
Agreed by SMT	June 2022
Review date	June 2024

1. Introduction.....	3
2. Policy Framework.....	3
3. Scope.....	3
4. Responsibilities.....	3
5. Policy.....	4
6. Appointing Processors.....	6
7. Monitoring.....	6
8. Implementation and Review.....	7
9. Approval.....	7
10. Change History.....	8
Appendix A: Processor and Sub-Processor Questionnaire.....	9
Appendix B: Processor and Sub-Processor Monitoring Plans.....	19

1. Introduction

- 1.1 This is a Policy of Age UK East London (“the Company”), registered in England as a private Limited Company by guarantee without share capital use of 'Limited' exemption under No. 07687015 and as Charity No. 1144535 (“the Company”).
- 1.2 This document sets out the Company’s Policy regarding its arrangements for employing external suppliers to process Personal Data:
 - a) Directly as Processors for the Company as the Controller of the Personal Data;
 - b) Indirectly as Sub-Processors sub-contracted by the Company’s Processors
 - c) as Sub-Processors, where the Company is a Processor for another Controller’s Personal Data.
- 1.3 The document also contains Appendices that contain:
 - A. A Questionnaire to be completed by Processors and Sub-Processors
 - B. A Monitoring Plan followed by the Company

2. Policy Framework

- 2.1 This Policy is part of the Company's Data Security and Protection Policy Framework.
- 2.2 This Policy should be interpreted in conjunction with the Company’s primary policy in the Framework, the Data Security and Protection Policy.
- 2.3 Definitions and abbreviations contained in the Company’s Data Security and Protection Policy apply equally to this Policy.

3. Scope

- 3.1 All policies and procedures set out in this document must be followed at all times by the Company, its employees, agents, contractors, volunteers and other parties (“Parties”) acting or working on its behalf.

4. Responsibilities

- 4.1 The Company’s **Senior Information Risk Officer** (SIRO) is responsible for:
 - a) making arrangements to ensure the security and integrity of Personal Data processed by the Company’s Processors and Sub-Processors
 - b) ensuring that all Parties are kept aware of the requirements of this Policy and of all related legislation, regulations, and other relevant rules whether now or in the

future in force including, but not limited to, the Data Protection Legislation and the Computer Misuse Act 1990

- c) Assessing the information risks of employing Processors and Sub-Processors, especially when appointing new suppliers
- d) maintaining a Processor and Sub-Processor Monitoring Plan to ensure proper scrutiny and management of data protection in its Processors and Sub-Processors
- e) arranging audits of compliance with this Policy by the Company's Processors and Sub-Processors

4.1 The Company's **Data Protection Officer** ("DPO") is responsible for:

- a) advising and assisting the Company in performing:
 - i) Data Processing Threshold Assessments
 - ii) assessment of responses to the Processor and Sub-Processor Questionnaire
 - iii) other checks prior to approving or continuing to use the Processors and Sub-Processors employed by the Company.
 - iv) inspections of the premises of Processors and Sub-Processors where practical and deemed necessary
- b) assisting the Company with auditing compliance with this Policy by its Processors and Sub-Processors

5. Policy

5.1 The Company shall only employ Processors under written contracts or legally binding Data Processing Agreements containing approved terms relating to Processing

5.2 The Company shall only employ Processors or Sub-Processors to process Personal Data outside of the UK where at least one of the following pertains:

- a) the country or territory to which the Personal Data is to be exported is within the European Economic Area (EEA)
- b) the country or territory to which the Personal Data is to be exported is one for which the UK regards as adequate in relation to its Data Protection provisions. *See footnote:* ¹

¹ Currently (although subject to change)

The EU States: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg,

- c) the rights and freedoms of Data Subjects are protected by legally binding contract terms, security and other safeguards, agreed between the Company and the Processors or Sub-Processors, that provide a level of protections at least are equal or equivalent to those afforded by the UK; or
 - d) a specific exception or arrangement between the Company and the Processor or Sub-Processor has been approved by the Information Commissioner or other relevant supervisory authority.
- 5.3 The Company shall only engage with Processors or Sub-Processors able to provide adequate security, including technical, physical and organisational security.
- 5.4 Contracts with Processors or Sub-Processors will expressly set out the service(s) to be provided, require the Processors or Sub-Processors to provide suitable security for the Personal Data to be processed and require that all Personal Data will be either destroyed or returned to the Company upon the termination of the Contract.
- 5.5 In the context of the preceding paragraphs, the Company has a preference for Processors and Sub-Processors with formal certifications in cyber security e.g. Cyber Essentials, Cyber Essentials Plus or ISO 27001.
- 5.6 Processors and Sub-Processors without formal cyber security certifications will be expected to demonstrate compliance with the National Cyber Security Centre's '10 Steps to Cyber Security'.
- 5.7 Where the Company employs Sub-Processors to process Personal Data on behalf of other Controllers, it will ensure that they comply with the requirements of the relevant Controllers and facilitate direct contact between them and those Controllers as required.
- 5.8 The Company reserves the right to grant or withdraw approval of the employment of its Processors as well as Sub-Processors acting on behalf of its Processors. It will exercise this right where Processors or Sub-Processors fail to meet the required standards.

Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, The EFTA States: Iceland, Norway and Liechtenstein. In addition: Gibraltar, Countries, territories and sectors covered by the European Commission's adequacy decisions i.e. Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. Additionally, Japan – only private sector organisations and Canada - only data subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).

6. Appointing Processors

- 6.1 Before formally appointing a Processor or direct Sub-Processor, the Company will, under advice from and the supervision of the Company's DPO:
- a) carry out or update:
 - i) a Data Protection Threshold Assessment taking into account the employment of the Processor or Sub-Processor or;
 - ii) an alternative form of information security risk assessment taking into account the employment of the Processor or Sub-Processor;
 - b) undertake a full DPIA if the DPIA Threshold Assessment or alternative risk assessment indicate that one is required under Data Protection Law or is otherwise advisable or desirable;
 - c) undertake audits of the potential Processor or Sub-Processor's security arrangements if, taking into account the nature of the Personal Data to be processed and the specific circumstances of the Data Processing (e.g. where sensitive Personal Data to be processed), the Company's DPO deems it necessary;
 - d) where the Company's DPO deems it necessary, require the potential Processor or Sub-Processor to complete, a *Processor and Sub-Processor Questionnaire* (a template of which is attached to this document within Appendix A); and
 - e) where the Questionnaire responses reveal that the potential Processor or Sub-Processor does not have suitable cyber security certification, require the potential Processor or Sub-Processor to demonstrate that they conform to the National Cyber Security Centre (NCSC)'s '10 steps to Cyber Security'.
 - f) Draw up a contract and/or legally binding Data Processing Agreement, to be entered into with the potential Processor or Sub-Processor. This must contain suitable clauses relating to the Processing of Personal Data and require the Processor or Sub-Processor to obtain expressed written permission from the Company before employing Sub-Processors.
- 6.2 Potential Processors and Sub-Processors that do not meet the required standards may be unable to undertake Processing or Sub-processing on behalf of the Company, at least until they are able to reach the required standard.

7. Monitoring


- 7.1 The Company will add the details of newly appointed Processors and Sub-Processors to its Processors and Sub-Processors Monitoring Plans, attached to this document as Appendix B.
- 7.2 The Company will regularly undertake the checks contained in its Monitoring Plans in accordance with the advice and guidance of its Data Protection Officer.

8. Implementation and Review

- 8.1 This Policy and Procedures shall be deemed effective as of 27th June 2022. No part of this document shall have retroactive effect and shall thus apply only to matters occurring on or after this date.
- 8.2 This document will be reviewed regularly and normally at least every two years.
- 8.3 This document will be updated as necessary to reflect current best practice, official guidance, and in line with current legislation.
- 8.4 The latest version of this document will be made readily available to all Staff, the Company's Processors and Sub-Processors and other relevant parties.

9. Approval

This Policy and Appendices have been approved and authorised by:

Name:	Geetha Umaasuthan
Position:	Director of Finance and Operations
Date:	27/06/2022
Due for Review by:	26/07/2024
Signature:	

10. Change History

Version	Section	Issue	Change	Approval	Date
4.0	All	Review of whole document	Minor	DPO	24/06/2022
4.0	Appendix B	Added Exigia Ltd	Plan completed	DPO	24/06/2022
4.0	5.2 b)	Update of adequate territories	Text slightly reworded and footnote list updated	DPO	24/06/2022
3.0	All	New document framework	Major update with the incorporation of the previously separate Questionnaire and Monitoring Plans as Appendices.		
3.1	Appendix A	10 Steps to Cyber Security	Added an NCSC Infographic and Section No 11 for response		

Appendix A: Processor and Sub-Processor Questionnaire

Background

- The UK GDPR applies to Controllers (who say how and why Personal Data is processed) and to Processors (who process Personal Data on behalf of a Controller under a contract or legally binding Data Processing Agreement).
- Where a Processor is permitted to sub-contract the processing of Personal Data it was employed by the Company to process, that sub-contractor will become a Sub-Processor.
- Processors and Sub-Processors are expected to maintain the same standards in relation to the processing and security of Personal Data as those that apply to their Controllers and Processors respectively.
- Sub-Processors thus employed must be bound by a suitable contracts or legally binding Data Processing Agreements containing the same or equivalent terms relating to Processing Personal Data as the contract between the Company and the Processor.

Questionnaire Notes

1. This Questionnaire supports Age UK East London's *Data Processing by External Suppliers Policy*.
2. The purpose of this Questionnaire is to assess whether potential Processors and Sub-Processors:
 - a. meet the requirements of the Data Protection Legislation under which Processors and Sub-Processors now have direct legal obligations and penalties can be imposed by the Information Commissioner's office (ICO);
 - b. meet the National Cyber Security Centre (NCSC)'s standards set out in its "10 Steps to Cyber Security".
 - c. and meet the Company's standards in protecting the rights of its Data Subjects and those of its Controllers and partners.
3. Potential Data Processors and Sub-Processors should answer all questions.
4. The assessment of responses will be undertaken by Age UK East London.
5. Potential Data Processors and Sub-processors that do not meet the required standard may be unable to undertake processing of Personal Data on behalf of the Company, at least until they are able to reach the required standard.
6. Potential Data Processors and Sub-processors should note that:
 - a. Data Processors and Sub-processors will be expected to manage their own costs in relation to completing this Questionnaire and any other assessment requirements required by the Company and for compliance with Data Protection legislation

- b. If they fail to meet the required standard they may be unable to undertake processing of Personal Data on behalf of the Company, at least until they are able to reach the required standard.
- c. If the contract documents to be entered into by a Data Processor or Sub-processor do not in themselves adequately describe its obligations relating to the Processing of Personal Data in the judgement of Age UK East London, the Parties will need to enter into an additional legally binding Data Processing Agreement.

No	Question	Response	Guidance	Score
1	<p>Policies & Records Provide evidence of your policies and procedures to inform staff of their responsibilities and set out your organisation's standards in:</p> <ul style="list-style-type: none"> • Data Protection • Information Security • Records Management • Subject Access Requests • Data Disposal • Data Backup • Business Continuity and Disaster recovery 	<p>Provide attachment(s) Data Backup /Business Continuity and Disaster recovery plan/policy ICT back up and how service will operate if ICT fails / needs recovery or lack of access to buildings</p>	<p>Policies should cover:</p> <ul style="list-style-type: none"> • Data Protection Clear details setting out how data is kept safe, the limits to access data, roles and responsibilities, guidance for handling data • Information Security Premises security, access to ICT systems, ICT security, Records Management What records are kept, who can access them, how to record, safe data transfer • Subject Access Request Procedure Staff and user awareness, process, roles and responsibilities defined. Arrangements for Sub-Processors • Data Disposal Procedure/policy retention period, safe disposal e.g. shredding or secure waste bins, electronic records, end of contract process. 	<p>Scored: [1] [2] [3] [4] [5]</p>

No	Question	Response	Guidance	Score
2	Do you assess data / privacy risks? How?	[Yes] or [No] Provide details and/or attachment(s)	Use of privacy impact assessment for new data processing / willing to use template for this contract	[Pass]/[Fail] Scored: [1] [2] [3] [4] [5]
3	Do you keep a central record of data processing activities?	[Yes] or [No] Provide details and/or attachment(s)	<ul style="list-style-type: none"> • The record should set out data processed, purpose, condition for processing, responsible person, any ICT system, retention period • If more than one, one entry for each process • NB if this contract delivers a new process for supplier, they will need to show example • Should be reviewed once a year (minimum) 	[Pass]/[Fail] Scored: [1] [2] [3] [4] [5]
4	What are your policies and procedures for dealing with security incidents / data breaches?	Provide details and/or attachment(s)	Clear process: who to report to, who will investigate, evaluation of the incident and resolution, e.g. lost file, computer virus	Scored: [1] [2] [3] [4] [5]

No	Question	Response	Guidance	Score
5	<p>Staff Training and Awareness Does everyone in your organisation receive appropriate training and awareness briefings on data protection and information security including?</p> <ul style="list-style-type: none"> • The Board • Senior management • Specialist Security staff • IT staff • All other staff <p>Please describe the nature of the training given, when it is given and who is responsible for carrying it out.</p>	<p>[Yes] or [No]</p> <p>Provide details and/or attachment(s)</p>		<p>Scored: [1] [2] [3] [4] [5]</p>

No	Question	Response	Guidance	Score
<p>6 (See also 11)</p>	<p>Organisational and Technical Measures to protect Personal Data Please provide evidence that you have a level of ICT security appropriate to the risk, taking into account the harm which might result from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.</p>	<p>[Yes] or [No]</p> <p>Provide details and/or attachment(s)</p> <p>Alternatively:</p> <p>Provide a summary of your '10 Steps' approach in Section No 11 below.</p>	<p>ICT security controls are in place to prevent accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access</p> <p>Accreditation / Certification is desirable: e.g. Cyber Essentials, Cyber Essential Plus, ISO27001, IASME Governance.</p> <p>Alternatively:</p> <p>If your organisation is not accredited or certified, demonstrate your compliance with the National Cyber Centre (NCSC)'s '10 Steps to Cyber Security' at Section No 11 below.</p>	<p>[Pass]/[Fail]</p>
<p>7</p>	<p>Location of Data Confirmation of where electronic data is (to be) held [in house or off-site and in which country or territory]</p>	<p>[onsite] or [offsite] Also specify location(s)</p>		<p>Information only</p>

No	Question	Response	Guidance	Score
8	<p>Backups Do you regularly back-up data?</p>	<p>[Yes] or [No] Provide details and/or attachment(s)</p>	<p>Systems back up/ business continuity appropriate to type of data</p> <ul style="list-style-type: none"> • Paper records • Cloud storage 	<p>[Pass]/[Fail] and Scored: [1] [2] [3] [4] [5]</p>
9	<p>Data Transfers Do you transfer personal data?</p> <p>If so, explain how data is transferred?</p> <p>Please confirm that all personal data processing occurs within the EEA or countries/territories about which the UK has made a positive adequacy decision.</p>	<p>[Yes] or [No] Provide details and/or attachment(s)</p>	<p>e.g. Encrypted email, tracked post for special category data e.g. where are your tools such as SurveyMonkey / Mail Chimp and Google Analytics hosted</p>	<p>[Pass]/[Fail] (if applicable) and Scored: [1] [2] [3] [4] [5]</p>

No	Question	Response	Guidance	Score
10	<p>Monitoring Mechanisms for Compliance with the General Data Protection Regulation is assessed at least annually.</p> <p>For example,</p> <ul style="list-style-type: none"> • Information Security audits • Records Management audit • Business Continuity and Disaster recovery plan tested • Formal accreditation or certification e.g. NHS Data Security & Protection Toolkit, IASME Governance 	<p>[Yes] or [No]</p> <p>Provide review plans and other details and/or attachment(s)</p>	<p>You should have plans in place to conduct audits of the information or processes relating to your compliance with Data Protection Legislation</p>	<p>[Pass]/[Fail] and Scored: [1] [2] [3] [4] [5]</p>
11 (See also 6)	<p>The 10 areas (Steps) to be used as headings under which to provide your response are:</p> <ol style="list-style-type: none"> 1. Risk management 2. Engagement and training 3. Asset management 4. Architecture and configuration 5. Vulnerability management 6. Identity and access management 7. Data security 8. Logging and monitoring 9. Incident management 10. Supply chain security 		<p>This section only needs to be completed if your organisation does not have an appropriate accreditation or certification - See Section No 6 above.</p> <p>See the NCSC <i>infographic</i> below and for more detailed guidance behind the '10 Steps', refer to the NCSC website at:</p> <p>https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security</p>	<p>[Pass]/[Fail]</p>



10 Steps to Cyber Security

This collection is designed for security professionals and technical staff as a summary of NCSC advice for medium to large organisations. We recommend you start by reviewing your approach to risk management, along with the other nine areas of cyber security below, to ensure that technology, systems and information in your organisation are protected appropriately against the majority of cyber attacks and enable your organisation to best deliver its business objectives.

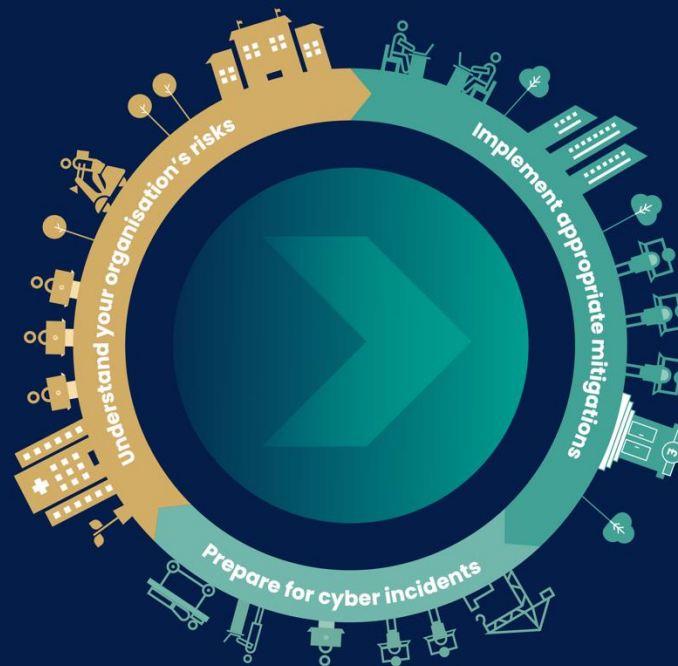
➤ **Risk management**
Take a risk-based approach to securing your data and systems.

➤ **Engagement and training**
Collaboratively build security that works for people in your organisation.

➤ **Asset management**
Know what data and systems you have and what business need they support.

➤ **Architecture and configuration**
Design, build, maintain and manage systems securely.

➤ **Vulnerability management**
Keep your systems protected throughout their lifecycle.



➤ **Identity and access management**
Control who and what can access your systems and data.

➤ **Data security**
Protect data where it is vulnerable.

➤ **Logging and monitoring**
Design your systems to be able to detect and investigate incidents.

➤ **Incident management**
Plan your response to cyber incidents in advance.

➤ **Supply chain security**
Collaborate with your suppliers and partners.



**Age UK East London
Processor and Sub-Processor Monitoring Plan**

**Appendix B:
Processor and Sub-Processor Monitoring Plans**

- These plans are produced and updated with the advice and guidance from the Company's Data Protection Officer.
- The Company will add the details of newly appointed Processors and Sub-Processors to these Plans.
- The Company will regularly undertake the checks contained in its Monitoring Plans with the advice and guidance of its Data Protection Officer.

Age UK East London Processor and Sub-Processor Monitoring Plan

Supplier (Service) (Role)	Action	Date	Next Planned Date	Status Notes
Safetynet IT Ltd. Supplier of: IT Support Processor: Processing Personal Data controlled by the Company	DPIA Threshold Assessment	n/a	n/a	
	Review contract(s) and / or DPAs	17/06/2021	31/01/2022	
	Check use of Sub-Processors	30/06/2021	31/01/2022	
	Check cyber security accreditation status	17/06/2021	30/06/2021	Working on Cyber Essentials Pro application Proving a long process due to the many customer networks they access
	Complete Questionnaire	n/a	n/a	
	Compliance with NCSC 10 steps to Cyber Security	30/06/2021	31/08/2020	
	Check for Personal Data breaches	19/06/2021	31/01/2022	None

Age UK East London Processor and Sub-Processor Monitoring Plan

Supplier (Service) (Role)	Action	Date	Next Planned Date	Status Notes
Dizons Ltd. Supplier of Charitylog CRM etc. Processor: Processing Personal Data controlled by the Company	DPIA Threshold Assessment	n/a	n/a	
	Review contract(s) and / or DPAs	30/09/2020	31/01/2022	
	Check use of sub-processors	30/06/2020	31/01/2022	
	Check cyber security accreditation status	01/03/2020	31/01/2022	Cyber Essentials Pro accreditation to 28/02/2021
	Complete Questionnaire	n/a	31/01/2022	
	Compliance with NCSC 10 steps to Cyber Security	n/a	31/01/2022	
	Check for Personal Data breaches	19/06/2021	31/01/2022	None

**Age UK East London
Processor and Sub-Processor Monitoring Plan**

Supplier (Service) (Role)	Action	Date	Next Planned Date	Status Notes
Advantage Services (Europe) Ltd. Supplier of: Sage Finance & Payroll, HR Systems. Processor: Processing Personal Data controlled by the Company	DPIA Threshold Assessment	30/06/2020	n/a	
	Review contract(s) and / or DPAs	30/06/2020	31/01/2022	
	Check use of sub-processors	30/06/2020	31/01/2022	Uses INS data centre
	Check cyber security accreditation status	31/03/2020	31/01/2022	Preparing an application for Cyber Essential Pro
	Complete Questionnaire	n/a	31/01/2022	
	Compliance with NCSC 10 steps to Cyber Security to Cyber Security	12/03/2020	31/01/2022	12/03/20 Provided a comprehensive response to our query and have demonstrated to us their compliance with NCSC 10 steps to Cyber Security
	Check for Personal Data breaches	19/06/2021	31/01/2022	None

**Age UK East London
Processor and Sub-Processor Monitoring Plan**

Supplier (Service) (Role)	Action	Date	Next Planned Date	Status Notes
Exigia Ltd. Supplier of: Information Governance Services and Training Processor: Processing Personal Data controlled by the Company	DPIA Threshold Assessment	n/a	n/a	
	Review contract(s) and / or DPAs	01/04/2021	01/04/2023	Adequate
	Check use of sub-processors	20/06/2022	01/06/2023	Checked
	Check cyber security accreditation status	n/a	n/a	n/a
	Complete Questionnaire	20/06/2022	01/06/2023	Adequate
	Compliance with NCSC 10 steps to Cyber Security to Cyber Security	20/06/2022	01/06/2023	Complies
	Check for Personal Data breaches	20/06/2022	01/06/2023	None