Agreement Relating to Data Processing

SERVICE/SOLUTION: MES Engage, Recruit, Research and Project Management Services

CLIENT: North East Hampshire and Farnham CCG on behalf of FRIMLEY HEALTH AND CARE INTEGRATED CARE SYSTEM (ICS)

DATE OF AGREEMENT:- 26th June 2019

Unless otherwise agreed in writing between the Parties, the agreed date for data to be provided to MES as outlined in the relevant MES Project Setup documentation and ongoing intervals as determined by the Client.

PARTIES

Frimley Health and Care ICS whose registered office is at NHS North East Hampshire & Farnham Clinical Commissioning Group Aldershot Centre for Health, Hospital Hill, Aldershot, Hampshire, GU11 1AY ("**Data Controller**"); and

(1) Membership Engagement Services Limited **(MES)** whose registered office is at 33 Clarendon Road, London, N8 0NW ("**Data Processor**")

The Data Processor agrees to store and process the personal data outlined below in accordance with the terms of this Agreement contained in Schedule 1.

Type and categories of personal data to be processed:	Personal Data is public and/or citizens panel membership data as detailed below.
Project for which processing of personal data is required:	For the recruitment, collection, retention, ongoing engagement, research, analysis, feedback, reporting and maintenance of the Client's citizens panel membership as per the requirements set out in the Client's public task or Terms of Reference. This includes mailings, online surveys, postal surveys, telephone surveys, face to face meetings, focus groups and participating in workshops.
Purpose of processing of personal data:	The Personal Data will be processed for the purposes of retaining and maintaining a citizens panel membership as part of the Client's public task. Personal data will also be processed for communication and engagement purposes such as inviting citizen panel members to take part in online surveys, postal surveys, attend face to face meetings, focus groups and participating in workshops. The data collected from engagement activities will be processed for research purposes only and will only be used to provide feedback on health and care services in the Frimley Health and Care ICS area. The purpose of processing the Personal Data is to engage and collect information on residents' views around health and care in the Frimley Health and Care ICS area. Collecting this information is also necessary to ensure that the panel remains representative of the local population.
Personal data to be collected:	Personal Data is citizens panel membership data consisting of title, full name, address, email address, telephone number and other communication channel data and preferences, ethnicity, date of birth, socio demographic information, disability, sexual orientation, language preferences, membership level of involvement preferences and other sensitive personal data deemed to be required by the Client for analysis and reporting

	purposes, interests and connection/relationship with the organisation.
Disposal and destruction of personal data	As agreed in writing between the parties should the contract be terminated.
Subcontractors required (where personal identifiable data may be shared)	- CACI: for demographic data appendage - Data8: for the purposes of carrying out data cleansing tasks - Qualtrics: for the purposes of administering surveys and analysing data - Pansensic: for the purposes of analysing data - Plus Four Market Research ltd: for the purposes of generating cross tabulations for data analysis - Blue Fire Coding: for the purposes of open text/free text comment analysis - Amazon SES: for the purposes of delivering emails through the ClickEmail function - DocMail: for the purposes of delivering mail through the ClickPost function - BCH: for the purposes of delivering SMS texts through the ClickText function

This agreement will cease at the point the service/solution is not continued with MES, shutdown of the solution is complete and all data pertaining to it is removed and securely destroyed, with written confirmation of that having occurred provided by MES to the Client (Data Controller).

The ERS Group Data Protection Officer is Ian Robinson. He can be contacted via dpo@theersgroup.com.

Signed on Behalf of Membership Engagement Services Limited:

Name Nick Goodman
Title Managing Director

Signed on behalf of Frimley Health and Care ICS

Name
Title

Dated:

Schedule 1: Terms of Agreement relating to Data Processing

1 DEFINITIONS AND INTERPRETATION

1.1 In this Agreement the following expressions bear the following meanings unless the context otherwise requires:

"**Agreement**"	means this data processing agreement between the Data Controller and Data Processor.
"**Confidential Information**"	means all proprietary and confidential information of a party or Personal Data which by its very nature should be treated as confidential or which is designated as confidential by a party, including: • information relating directly or indirectly to the Data Controller's business, including details of trade secrets, know-how, plans, strategies, ideas, operations, compliance information, processes, methodologies and practices • information relating directly or indirectly to the Data Controller's customers, suppliers or business partners (or potential customers, suppliers or business partners) • works of authorship, products and materials written and prepared by or on behalf of the Data Controller, software, data, diagrams, charts, reports, designs, specifications, inventions and working papers or similar materials of whatever nature and on whatever media; and • the provisions of this Agreement.
"**Data Privacy Laws**"	means all laws that relate to data protection, privacy, the use of information relating to individuals, and or the information rights of individuals including without limitation, the Data Protection Act 2018, the Privacy and Electronic Communication (EC Directive) Regulations 2003, the Regulation of Investigatory Powers Act 2000, the Telecommunications (lawful Business Practice) (Interception of Communications) Regulations 2000, Privacy and Electronic Communications (EC Directive) Regulations 2003, the Consumer Protection from Unfair Trading Regulations 2008, any laws in force in any relevant jurisdiction which implements the Directive, the Regulation, and all and any regulations made under those acts or regulations all applicable formal or informal guidance, rules, requirements, directions, guidelines, recommendations, advice, codes of practice, policies, measures or publications of the Information Commissioner's Office, other relevant regulator, and or relevant industry body, in each case in any relevant jurisdiction(s) and the equivalent in any other relevant jurisdictions.
"**Data Processor Personnel**"	means all staff, contractors, employees, agents, sub-contractors and sub-processors of the Data Processor
"**Data Subject**"	has (until 24 May 2018) the meaning given under the Directive and (from 25 May 2018) the meaning given under the Regulation
"**Directive**"	means the European Commission Directive 95/46/EC with respect to the Processing of Personal Data
"**Personal Data**"	means any information relating to an identified or identifiable natural person ('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. The nature of some of the data collected is sensitive.
"**Processing**"	means obtaining, recording or holding Personal Data or carrying out any operation or set of operations on Personal Data (whether or not by automatic means), including: (a) organisation, adaptation or alteration of Personal Data; (b) retrieval, consultation or use of Personal Data; (c) disclosure of the information or Personal Data by transmission, dissemination or otherwise making available; or

	(d) alignment, combination, blocking, erasure or destruction of the Personal Data, (e) and "**Processed**", "**Processes**" and "**Process**" shall be construed accordingly.
"**Regulation**"	means the Data Protection Act 2018 and the General Data Protection Regulations (GDPR)
"Supervisory Authority"	means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Privacy Laws;

1.2 Headings contained in this Agreement are for reference purposes only and shall not be incorporated into this Agreement and shall not be deemed to be any indication of the meaning of the clauses or sub-clauses to which they relate.

1.3 References to the singular include the plural (and vice versa) and words denoting persons include individuals, bodies corporate, partnerships, unincorporated associations and other bodies.

1.4 A reference to a statute, statutory provision or any subordinate legislation shall unless otherwise stated be construed as including a reference to that statute, provision or subordinate legislation as in force at the date of this Agreement and as amended, extended, re-enacted or replaced from time to time.

1.5 The schedules form part of this Agreement and references to this Agreement include the schedules.

1.6 References to clauses and schedules are to clauses of and schedules to this Agreement; references in a schedule to paragraphs are to the paragraphs of that schedule; and a reference to a clause or paragraph number is, unless otherwise specified, a reference to all its sub-clauses or sub-paragraphs.

1.7 In this Agreement the words "other", "includes", "including" and "in particular" do not limit the generality of any preceding words and any words which follow them shall not be construed as being limited in scope to the same class as the preceding words where a wider construction is possible.

2 DATA CONTROLLER

2.1 The Data Processor acknowledges that the Data Controller shall solely be responsible for the following decisions and determinations:

(a) the purpose(s) for which and the manner in which the Personal Data will be Processed or used;
(b) what Personal Data to collect and the legal basis for doing so;
(c) which items (or content) of Personal Data to collect;
(d) which individuals to collect Personal Data about;
(e) whether to disclose the Personal Data, and if so, who to;
(f) whether subject access and other individuals' rights apply including the application of any exemptions;
(g) how long to retain the Personal Data; and
(h) whether to make non-routine amendments to the Personal Data.

3 CONTROLLER'S INSTRUCTIONS

3.1 The Data Processor shall only Process Personal Data on behalf of the Data Controller in accordance with instructions issued by the Data Controller from time to time. The Data Processor agrees to Process all such Personal Data in accordance with Data Privacy Laws and the provisions of this Agreement.

4 TECHNICAL, SECURITY AND ORGANISATIONAL MEASURES

4.1 The Data Processor shall, having regard to the state of technological development, take all appropriate technical, security, and organisational measures necessary or desirable in relation to the Processing of Personal Data under this Agreement which shall as a minimum include the following measures:

(a) prevent unauthorized persons from gaining access to data processing systems with which Personal Data are Processed;
(b) prevent the Data Processor's systems from being Processed without authorisation;
(c) ensure that persons entitled to use a data processing system have access only to the Personal Data to which they have a right of access;
(d) ensure that Personal Data cannot be read, copied, modified or removed without authorization during any Processing;
(e) ensure that it is possible to check and establish whether and by whom Personal Data has been input into data processing systems, modified or removed; and
(f) ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful Processing or accidental loss, destruction or damage and the nature of the Personal Data to be protected which shall include, as a minimum the measures set out in Schedule 2 (Security, Technical and Operational Measures).

4.2 The Data Processor shall upon written request from the Data Controller from time to time inform the Data Controller of the measures it has taken to comply with clause 4.1 above, and the Data Processor will at its own cost implement any further steps that are necessary for compliance with clause 4.1. The Data Processor shall inform the Data Controller

promptly of any proposed changes to the security, technical and organisational measures which are detailed in Schedule 2 of this Agreement.

5 INFORMATION AND AUDIT

5.1 The Data Processor shall, during the term of this Agreement:

(a) permit without charge, on an annual basis, and / or where the Data Controller becomes aware of a Data Breach or alleged or potential breach of Data Privacy Laws (Data Protection Act 2018 and the General Data Protection Regulation (GDPR) by the Laws by the Data Processor, reasonable access by the Data Controller or any regulator to all records, files, tapes, premises, equipment, facilities, audit, security and IT reports, computer systems, or any other information howsoever held by the Data Processor in respect of the Data Processor's activities pursuant to this Agreement, for the purposes of reviewing compliance with the Data Privacy Laws Data Protection Act 2018 and the General Data Protection Regulation (GDPR)

(b) provide without charge all reasonable assistance to the Data Controller or any regulator in complying with any direction, requirement or request made by any regulator to do or not to do any act, or to provide any information in respect of any obligation of the Data Processor under this Agreement, including, where necessary, giving the regulator (including its representatives or appointees) reasonable access to any records, files, tapes, computer systems, or any other information howsoever held.

5.2 For the purpose of this clause 5, **reasonable access** shall mean as a minimum, access on not less than 48 hours' notice and during normal working hours and access to all information held by the Data Processor and in the event of an alleged or potential breach of Data Privacy Laws or this Agreement **reasonable access** shall mean access as soon as reasonably practicable.

5.3 The Data Processor agrees that the Data Controller may appoint a third party independent auditor to audit the Data Processor's compliance with this Agreement and the Data Privacy Laws Data Protection Act 2018 and and to determine the accuracy and completeness of the statements and records submitted by the Data Processor under this Agreement.

5.4 The exercise by the Data Controller of its rights of inspection in clauses 5.1 to 5.3 above shall not relieve the Data Processor of any of its obligations under this Agreement.

5.5 The Data Processor shall procure that any subcontractor shall permit the Data Controller to exercise equivalent rights of inspection and audit as set out in clauses 5.1 to 5.3 above in respect of services provided by such subcontractor.

6 PROCESSING OBLIGATIONS

6.1 The Data Processor shall not disclose Personal Data without the written consent of the Data Controller and only Process Personal Data on behalf of the Data Controller in accordance with:

(a) the purposes set out in this Agreement; and

(b) the express instructions received from the Data Controller from time to time

(except to the extent to which Data Protection Act 2018 and the General Data Protection Regulation (GDPR) or Union or Member State Laws require Personal Data to be Processed for other purposes in which case the Data Processor shall as soon as reasonably practicable and before the processing takes place inform the Data Controller of this requirement unless the law prohibits such disclosure on important grounds of public interest).

6.2 The Data Processor shall take steps to ensure that any Data Processing Personnel acting under their authority who has access to Personal Data does not process them except on instructions from the Data Controller, unless he or she is required to do so by Union or Member State law.

6.3 The Data Processor shall:

(a) provide the Data Controller or any relevant regulator with a copy of all Personal Data on demand;

(b) make all reasonable efforts to ensure that the Personal Data is accurate and up-to-date at all times; and

(c) not keep Personal Data for longer than is necessary in accordance with the Data Controller's instructions so as to comply with the principle of data minimisation.

7 COMPLIANCE WITH THE DATA PROTECTION ACT 2018 AND GENERAL DATA PROTECTION REGULATION

7.1 The Data Processor shall comply with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) without prejudice to the generality of the foregoing shall:

(a) at the request of the Data Controller or any relevant regulator, promptly make available to the Data Controller and/or any relevant regulator all information necessary to demonstrate compliance with the Data Processor's obligations and Data Protection Act 2018 and The General Data Protection Regulation (GDPR)

(b) not cause the Data Controller to be in breach of the Data Privacy Laws and shall use all reasonable endeavours to assist the Data Controller to comply with any obligations imposed on the Data Controller by the Data Protection Act 2018 and the General Data Protection Regulation (GDPR)

7.2 The Data Processor shall:

(a) assist the Data Controller by:

(i) complying with any requests by Data Subjects to exercise their rights under The Data Protection Act 2018 and The General Data Protection Regulation (GDPR) (including but not limited to their rights to access, or to cease or not begin processing, rectify, block, erase, destroy or object to the processing of their personal data, each a **Data Subject Request**);

(ii) ensuring that the Personal Data is deleted or corrected if it is incorrect (or, the Data Controller does not agree that it is incorrect, to have recorded the fact that the relevant person considers the

Personal Data to be incorrect within 5 (five) days' of being requested to do so by the Data Controller; and/or

(iii) communicating with or obtaining the approval of the Information Commissioner's Office (**ICO**) in relation to the Processing of Personal Data (**ICO Correspondence**);

including if so requested, providing a copy to the Data Controller of a Data Subject's Personal Data in a machine readable portable format.

(b) promptly, and in any event within forty-eight (48) hours of receipt of any request or correspondence, inform the Data Controller about the receipt of any Data Subject Requests or ICO Correspondence;

(c) not disclose any Personal Data in response to any Data Subject Request or ICO Correspondence, or respond in any way to such a request without first consulting with, and obtaining the consent of, the Data Controller unless obligated to do so by Union or Member State law; and

(d) assist the Data Controller should the Data Controller carry out a data protection impact assessment and shall provide the output of its own data protection impact assessment where relevant.

7.3 The Data Processor will (and will ensure that the Data Processor Personnel will) promptly (but in all cases within 48 hours) notify the Data Controller, if the Data Processor (or Data Processor Personnel as the case may be):

(a) becomes aware that a disclosure of Personal Data may be required under Data Privacy Laws;

(b) receives a complaint relating to the Data Controller's obligations under the Data Privacy Laws; and/or

(c) becomes aware of a breach of this Agreement.

7.4 In the event that the Data Processor believes that the Data Processor instructions conflict with the requirements of Data Privacy Laws, the Data Processor must inform the Data Controller immediately.

8 DATA BREACHES

8.1 The Data Processor shall:

(a) maintain a record of all categories of processing activities it undertakes under this Agreement in accordance with Data Protection Act 2018 and the General Data Protection Regulations (GDPR) and a record of any Data Breach (as defined below) and provide a copy of such record(s) to the Data Controller for inspection on demand;

(b) immediately (in order to meet the 72 hour window for reporting a breach) inform the Data Controller in writing of any unauthorized or unlawful processing of Personal Data and/or material incident of Personal Data loss, corruption, destruction, alteration, disclosure, access or damage ("**Data Breach**") or any action that causes or could reasonably be deemed to cause a Data Breach and shall liaise with the Data Controller in managing such Data Breach (including by providing sufficient information, cooperation, analysis and support);

(c) provide the Data Controller with such co-operation (at no additional cost to the Data Controller) in relation to the (i) Data Controller notifying the individual or the Information Commissioner (or relevant regulator) of the Data Breach, including by providing the Data Controller with a detailed description of the nature of the Data Breach and the identity of the affected person(s) and (ii) Data Controller's efforts to investigate, remediate, and mitigate the effects of any Data Breach; and

(d) shall not make any public announcement regarding such incident as set out in this clause 8.1 without prior consultation with the Data Controller and subject to the Data Controller's written consent.

9 TRANSFER OF PERSONAL DATA OUTSIDE EEA

9.1 The Data Processor shall not transfer Personal Data which has been obtained by or made available to the Data Processor to any country outside the European Economic Area (EEA) without the prior written consent of the Data Controller, such consent may be subject to and given on such terms as the Data Controller may in its absolute discretion prescribe.

9.2 In the event that the Data Controller consents to the transfer of Personal Data from the Data Processor to a country outside of the EEA the Data Processor shall comply with the following additional provisions:

(a) the Data Processor shall confirm in writing:

(i) the Personal Data which will be transferred to and/or Processed outside of the EEA;

(ii) any sub-contractor or other third parties who will be processing and/or receiving Personal Data outside of the EEA;

(iii) how the Data Processor will ensure an adequate level of protection and adequate safeguards in respect of the Personal Data that will be processed in and/or transferred outside of the EEA so as to ensure the Data Controller's compliance with the Data Privacy Laws;

(b) the Data Processor shall comply with such other instructions and shall carry out such other actions as the Data Controller may notify in writing, including:

(i) incorporating standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) into this Agreement or a separate data processing agreement between the Parties; and

(ii) procuring that any sub-contractor or other third party who will be processing and/or receiving or accessing the Personal Data outside of the EEA either enters into:

(A) a direct data processing agreement with the Data Controller on such terms as may be required by the Data Controller; or

(B) a data processing agreement with the Data Processor on terms which are equivalent to those agreed between the Data Controller and the Data Processor relating to the relevant Personal Data transfer, and

in each case which the Data Processor acknowledges may include the incorporation of model contract provisions (which are approved by the European Commission as offering adequate safeguards under the Data Privacy Laws) and technical and organisation measures which the Data Controller deems necessary for the purpose of protecting Personal Data.

10 SUB-CONTRACTING

10.1 The Data Processor shall not sub-contract to any third party any of its obligations to Process Personal Data on behalf of the Data Controller unless all of the following provisions of this clause have first been complied with:-

(a) the Data Processor has supplied to the Data Controller full details of the proposed sub-contractor, the results of a thorough due diligence undertaken by the Data Processor (including a risk assessment of the sub-contractor's information governance related practices and processes) and such further information as the Data Controller may require to ascertain that such sub-contractor has the ability to comply with the provisions of this Agreement; and

(b) the Data Processor has obtained the prior written consent of the Data Controller; and

(c) the proposed sub-contractor has entered into a contract with the Data Processor substantially upon the terms of this Agreement.

11 CONFIDENTIALITY & PERSONNEL

11.1 The Data Processor shall keep the Confidential Information of the Data Controller confidential in perpetuity and, except as provided in this Agreement, shall not disclose such Confidential Information to any third party and shall not itself use or exploit such Confidential Information except as provided in this Agreement.

11.2 The Data Controller undertakes to keep confidential any Confidential Information of the Data Processor of which the Data Controller may become aware when carrying out the inspections under the provisions of clause 5.1 above.

11.3 The Data Processor shall ensure that its Personnel processing Personal Data are reliable and have received adequate training on compliance with the Data Processor's obligations under this Agreement and the Data Privacy Laws.

11.4 The Data Processor shall employ only Data Processor Personnel who have committed themselves to confidentiality or are under an obligation of confidentiality.

12 AMENDMENTS

12.1 In the event that Data Privacy Laws are amended or replaced by subsequent legislation or regulations or in the event that case law pursuant to Data Privacy Laws and/or regulations enacted under it require amendments to this Agreement in the reasonable opinion of the Data Controller then the Data Processor will agree to such reasonable amendments to this Agreement and will enter into a deed of variation to effect such amendments.

13 APPLICATION OF AGREEMENT

13.1 The purpose of this Agreement is to deal with the effect of Data Privacy Laws on the Processing of Personal Data by the Data Processor on behalf of the Data Controller, and to ensure compliance with Data Privacy Laws. If, and to the extent that, any other contractual terms that have been agreed, or may in future be agreed, including any terms relating to liability and the rights and obligations between the Data Controller and the Data Processor conflict with the terms of this Agreement, the terms of this Agreement shall prevail except where such contractual terms are specifically expressed to vary the terms of this Agreement.

14 TERMINATION

14.1 The Data Controller and the Data Processor shall be entitled to terminate this Agreement forthwith by written notice in the event that the other party:

(a) is in material breach of its obligations under this Agreement; or

(b) prepares for or enters into any composition or arrangement with its creditors or an administration order or winding up order or similar process is presented against the Data Processor or Data Controller or an administrative receiver is appointed in respect of the business or part of the assets of the Data Processor or the Data Controller or either party forms the reasonable opinion that the other party has become or is likely in the immediate future to become unable to pay its debts within the definition of that term as set out in Section 123 of the Insolvency Act 1986.

14.2 Either party may terminate this Agreement by giving to the other party not less than one month's written notice to the other PROVIDED THAT subject to the provisions of clause 14.1 neither party may terminate this Agreement if following the date on which such termination shall take effect there will continue to be in force an agreement under which the Data Processor may be required to Process Personal Data on behalf of the Data Controller unless either that agreement or another agreement between the Data Controller and the Data Processor shall be in force to ensure compliance with Data Privacy Laws.

15 CONSEQUENCES OF TERMINATION

15.1 Upon termination of this Agreement in accordance with clause 14:-

(a) the Data Processor shall, at the Data Controller's option, either forthwith return to the Data Controller all copies of the Personal Data which it is Processing or has Processed upon behalf of the Data Controller, or securely destroy the same within 14 days of being requested to do so by the Data Controller unless the Data Processor is specifically required to retain the Personal Data by Data Privacy Laws or Union or Member State Laws; and

(b) the Data Processor shall cease Processing Personal Data on behalf of the Data Controller.

16 LAW AND JURISDICTION

16.1 This Agreement and any non-contractual obligations arising out of or in relation to this Agreement shall be governed by and construed in all respects in accordance with English law in every particular including formation and interpretation and shall be deemed to have been made in England, and each party hereby submits to the exclusive jurisdiction of the English courts in relation to all matters arising out of or in connection with this Agreement (whether contractual or non-contractual in nature).

17 GENERAL

17.1 For the purposes of this Agreement the "Data Controller" and the "Data Processor" shall include its affiliates, including but not limited to any subsidiaries (as defined by section 1159 of the Companies Act 2006) and any parent or associated undertaking.

17.2 Neither Party shall assign, charge, novate, subcontract or deal in any way with its rights or obligations under this Agreement without the prior written consent of the other Party.

17.3 The failure of either Party to enforce or to exercise, at any time or for any period of time, any term of or any right arising pursuant to this Agreement does not constitute, and shall not be construed as, a waiver of such term or right and shall in no way affect that Party's right to enforce or exercise it in the future.

17.4 No variation or amendment to this Agreement shall be effective unless agreed in writing by both Parties and signed by an authorised representative of both Parties.

17.5 The Parties intend each provision of this Agreement to be severable and distinct from the others. If a provision of this Agreement is held to be illegal, invalid or unenforceable, in whole or in part, the Parties intend that the legality, validity and enforceability of the remainder of this Agreement shall not be affected.

17.6 All notices and other such documents relating to the operation of this Agreement shall be delivered by hand or sent by first class registered pre-paid post to the respective addresses of the Parties stated at the beginning of this Agreement or to such other address as a Party may in writing notify to the other for the purpose of this clause.

17.7 This Agreement may be entered into in any number of counterparts and by the Parties on separate counterparts, all of which taken together shall constitute one and the same instrument.

SCHEDULE 2: Security, Technical and Operational Measures

1 Objective

1.1 This Schedule sets out the security, technical and organisational measures for protecting Personal Data against unauthorised access, corruption and loss processed by the Data Processor in connection with the services provided to the Data Controller.

2 Requirements

2.1 The Data Processor must ensure that industry standards for security and data protection are met as a minimum for the services provided to the Data Controller, including the protection of personal and confidential data. These standards include operating an information security framework and policy that aligns with the ISO 27001:2013 standard. Controls of particular significance that must be met are highlighted below.

3 Organisation of Information Security

3.1 Security resources in terms of structures and personnel with relevant skills and knowledge must be in place in order to ensure information security is effectively managed.

4 Vetting/recruitment

4.1 The Data Processor must have processes in place to undertake appropriate screening of Data Processor Personnel either prior to employment or before any access is given to Personal Data and a suitable record of those checks maintained (including any re-check carried out). The Data Controller may from time to time request evidence of up to date checks.

4.2 The checks must as a minimum include right to work in the UK (with further checks upon work permit expiry) for UK based Data Processor Personnel, basic Disclosure Barring Service Checks (full for FCA approved roles) and we reserve the right to request additional checks.

4.3 The Data Processor must ensure that all Data Processor Personnel have signed an appropriate confidentiality agreement.

4.4 When working at the Data Controller's locations or accessing the Data Controller's systems, the Data Processor Personnel and contractors must comply with the relevant policies as advised by the Data Controller's supervising manager. Where access to the Data Controller's systems is provided either onsite or remotely the Data Controller's HR team will perform vetting checks and the Data Controller shall obtain such necessary employee consents.

5 Training

5.1 The Data Processor must ensure that Data Processor Personnel undertake appropriate data protection and information security awareness training relevant to their work during induction (and before being given access to the Data Controller's premises and/or personal data) and at least annually thereafter and a suitable record maintained.

6 Disposal/destruction

6.1 The Data Processor must ensure that any Personal Data in a hard-copy format must be securely destroyed when no longer needed and securely disposed of via a certified waste service.

6.2 The Data Processor must ensure that a process is in place to securely destroy Data Controller's Personal Data so that it is unrecoverable from systems, portable computing devices and portable media prior to disposal. Records of destruction must be retained and made available to the Data Controller on request.

7 Access control (personal data / systems / buildings including offices, data centre)

7.1 The Data Processor must implement measures to prevent, detect and manage inappropriate and unauthorized access to all systems and physical locations that store, process or transmit the Data Controller's personal data in electronic and hard copy format. Access must be strictly controlled and restricted to only those Data Processor Personnel who are dedicated to delivering the services to the Data Controller and whose role requires them to have such access.

8 Data accuracy

8.1 The Data Processor must implement controls and quality checks to ensure that all outputs, for example, mailings and website content are accurate and strictly comply with the Data Controller's requirements.

9 Transfer control

9.1 The Data Processor must ensure that all electronic information transfer mechanisms used that contains Data Controller information are approved in advance by the Data Controller and are fully documented and secure. Transfers over public/non-secure networks must use industry standard encryption methods. Appropriate controls must be in place to protect any physical transfers of information.

10 Operational Security

10.1 The Data Processor will ensure formal procedures are implemented to manage technical threats, vulnerabilities and malware including applying vendor supplied security updates (patches) within recommended timeframes and anti malware products are installed, updated and maintained.

11 Sub contractors

11.1 Where the Data Processor has been authorised in writing by the Data Controller to engage sub-contractors (including members within the Data Processor's group) to provide some or all of the services, the provider will impose contractual obligations on the sub-contractor on terms substantially equivalent to those contained in this schedule.

12 Operational resilience

12.1 Arrangements and processes must be in place to prevent disruptions to service to the Data Controller and ensure the ability to respond quickly to, and recover from, a disruption should it occur.

13 Incident management

13.1 Appropriate mechanisms must be in place to promptly detect, report within agreed timescales and manage security incidents in order to minimise their impact, to learn from them and prevent recurrence.

14 Compliance

14.1 The Data Processor will ensure that periodic independent reviews are conducted, including annual penetration tests to provide assurance that key information security controls are operating effectively.

15 Data Protection Officer

15.1 The Data Processor has appointed a Data Protection Officer (**DPO**) Ian Robinson details on page 2..