

AGREEMENT RELATING TO DATA PROCESSING

Agreement start: 25th May 2018

PARTIES

- (1) **The Data Controller(s)** (see **SCHEDULE 3: DATA CONTROLLER(S)**) pertaining to the Local Authority ("**Data Controller(s)**"); and
- (2) **The ERS Group** (see **SCHEDULE 4: DATA PROCESSOR(S)**) and its subsidiary companies ("**Data Processor(s)**")

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: TERMS OF AGREEMENT RELATING TO DATA PROCESSING**.

Type and categories of Personal Data to be processed: "**Personal Data**" as detailed in **SCHEDULE 6: PERSONAL DATA**.

Project for which Personal Data processing is required: "**Projects**" as detailed in **SCHEDULE 5: PROJECTS**.

Purpose of processing of Personal Data: As detailed in **SCHEDULE 5: PROJECTS**.

Personal data to be collected: The "**Personal Data**" to be collected will be as detailed in **SCHEDULE 6: PERSONAL DATA**.

Disposal and destruction of Personal Data As agreed in writing between the parties or no later than 14 months from the end of the project to which the Personal Data relates.

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

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:

<p>"Agreement"</p>	<p>means this data processing agreement between the Data Controller and Data Processor.</p>
<p>"Confidential Information"</p>	<p>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:</p> <ul style="list-style-type: none"> • 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.
<p>"Data Privacy Laws"</p>	<p>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,</p>

	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
"Personal Data Breach"	has the meaning given to it in the Data Protection Act 2018
"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 General Data Protection Regulation ((EU) 2016/679)).
"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, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, take all appropriate technical, security, and organisational measures necessary 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 Personal Data Breach or alleged or potential breach of Data Privacy 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 and this Agreement; and
 - (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 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 Privacy Laws 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) subject to clause 10, 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 Data Privacy Laws

- 7.1 The Data Processor shall comply with the Data Privacy Laws and 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 Privacy Laws;
 - (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 Privacy Laws;
- 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 Privacy Laws (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.
 - (e) assist with consultations with Supervisory Authorities as required by Article 35 or 36 of the Regulation.
- 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 Privacy Laws and a record of any Personal Data Breach and provide a copy of such record(s) to the Data Controller for inspection on demand;



- (b) immediately inform the Data Controller in writing and, in any event, within the twenty-four (24) hour period after the Data Processor becomes aware of any Personal Data Breach or any action that causes or could reasonably be deemed to cause a Personal Data Breach and shall liaise with the Data Controller in managing such Personal 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 Data Subject 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 Personal Data Breach and the information referred to in Article 33(3)(b) to (d) of the Regulation and (ii) Data Controller's efforts to investigate, remediate, and mitigate the effects of any Personal 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 Privacy Laws) 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, andin 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 Voting Data

10.1 The following definitions and rules of interpretation apply in this section:

- (i) Voting Data: means all data that reflect the instructions, choices or opinions of the Data Subject collected by the Data Processor as part of the processes and procedures connected with this agreement,
- (ii) Electoral Software and Systems: means all software and systems that are used by the Data Processor for the purpose of the collection, tabulation and analysis of Voting Data.

10.2 The parties acknowledge and agree that, where it is not anonymous, Voting Data is Personal Data and the Data Controller shall, subject to clause 10.4, retain all rights, title and interest to the Voting Data.

10.3 The Data Processor shall:

- (a) at all times take appropriate technical and organisational measures against unauthorised or unlawful processing of Voting Data in accordance with this Agreement,
- (b) permit the Data Controller or the Data Controller's representative (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit, Electoral Software and Systems (and/or those of its agents and approved sub-contractors) and comply with all reasonable requests or directions by the Data Controller to enable the Data Controller to verify and/or procure that the Data Processor is in full compliance with its obligations under this Agreement.

10.4 The Data Controller shall:

- (a) undertake, subject to clause 10.4 (b) not to request access to the Voter Data unless it has been agreed in writing, prior to the collecting of Voter Data by the Data Processor, the purposes when access to the Voter Data will be provided by the Data Processor,
- (b) have access to the Voter Data for the purpose of a Data Subject Request,
- (c) require the Data Processor to retain the Voter Data for as long as specified in this agreement.

11 Sub-Contracting

11.1 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 (see **SCHEDULE 7: SUB-CONTRACTORS**); 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; and
- (d) the proposed sub-contractor is subject to periodic and 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.

11.2 In accordance with clauses 11.1 (a) and 11.1 (b) the Data Controller consents to the Data Processor sub-contracting to the sub-contractors listed in **SCHEDULE 7: SUB-CONTRACTORS**.

12 Confidentiality and Personnel

12.1 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.

12.2 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.

12.3 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.

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

13 Amendments

13.1 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.

14 Application of Agreement

14.1 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.

15 Termination

15.1 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.

15.2 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 15.1 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.

16 Consequences of Termination

16.1 Upon termination of this Agreement in accordance with clause 15:-

- (a) the Data Processor shall, at the Data Controller's option, either forthwith return to the Data Controller all copies of the Personal Data, but not Voting 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.

17 Law and Jurisdiction

17.1 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).

18 General

- 18.1 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.
- 18.2 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.
- 18.3 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.
- 18.4 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.
- 18.5 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.
- 18.6 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.
- 18.7 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 (see **SCHEDULE 7: 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.

SCHEDULE 3: DATA CONTROLLER(S)

It is understood that “**The Data Controller(s)**” represent the Local Authority and occupy at least one of the following positions:

"Data Controller(s)"
Returning Officer (“ RO ”)
Electoral Returning Officer (“ ERO ”)
Modern.Gov System Owner (“ SO ”)

SCHEDULE 4: DATA PROCESSOR(S)

It is understood that “**The Data Processor(s)**” within “The ERS Group” which service the Local Authority are as follows:

"Data Processor(s)"	Registered Office	Registered Number
Electoral Reform Services Limited (“ ERS ”)	33 Clarendon Road London N8 0NW	2263092
Modern Mindset Limited (“ MML ”)		02208130
Xpress Software Solutions Limited (“ XSSL ”)		4152280

SCHEDULE 5: PROJECTS

The Data Controller(s) (see **SCHEDULE 3: DATA CONTROLLER(S)**) instruct The Data Processor (see **SCHEDULE 4: DATA PROCESSOR(S)**) to process Personal Data (see **SCHEDULE 6: PERSONAL DATA**) on their behalf for the sole purpose of delivering the relevant projects described below, as required by individual Project Specifications.

1 Printing and distribution of poll cards

Data processor	Electoral Reform Services (“ERS”)
Project	Printing and distribution of poll cards.
Description of process	The process of facilitating the Data Controller in holding an election through the physical production and, where necessary, distribution of poll cards.
Reason for processing/collecting	The ERO has requested the use of this service and is legally obliged to conduct an election using printed and, in some cases, mailed materials.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of printing and distributing poll cards.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, fourteen months after the completion of the job.

2 Printing and distribution of postal ballot packs and polling station ballot papers

Data processor	Electoral Reform Services (“ERS”)
Project	Printing and distribution of postal ballot packs and/or polling station ballot papers.
Description of process	The process of facilitating the Data Controller in holding an election through the physical production and distribution of postal ballot packs and polling ballot papers.
Reason for processing/collecting	The ERO has requested the use of this service and is legally obliged to conduct an election using printed and mailed materials.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of printing and distributing postal ballot packs and polling ballot papers.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, fourteen months after the completion of the job.

3 Printing and distribution of forms and letters relating to electoral registration

Data processor	Electoral Reform Services (“ERS”)
Project	Printing and distribution of forms and letters relating to electoral registration.
Description of process	The process of facilitating the Data Controller in canvassing their electoral area through data processing (see Automated Household Response (AHR) service) and the physical production and, where necessary, mailing of Household Enquiry Forms (HEFs), Invitations to Register (ITRs), Household Notification Letters (HNLs) and other miscellaneous letters.
Reason for processing/collecting	The ERO has requested the use of this service and is legally obliged to conduct a canvass of their electoral area using printed and, in some cases, mailed materials.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of printing and distributing forms and letters relating to electoral registration.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, fourteen months after the completion of the job.

4 Printing and distribution of postal vote signature refresh letters

Data processor	Electoral Reform Services (“ERS”)
Project	Printing and distribution of postal vote signature refresh letters.
Description of process	The process of facilitating the Data Controller in holding an absent voter signature refresh campaign through the physical production and mailing of postal vote signature refresh letters and forms.
Reason for processing/collecting	The ERO has requested the use of this service and is legally obliged to conduct an absent voter signature refresh campaign through the physical production and mailing of postal vote signature refresh letters and forms.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of printing and distributing postal vote signature refresh letters.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, fourteen months after the completion of the job.

5 Printing and distribution of business improvement district (BID) canvass and notification of ballot letters

Data processor	Electoral Reform Services (“ERS”)
Project	Printing and distribution of business improvement district canvass and notification of ballot letters.
Description of process	The process of facilitating the Data Controller in notifying, and where necessary collecting the details of, ratepayers with regards to a forthcoming business improvement district ballot through the physical production and, where necessary, distribution of canvass and notification of ballot letters.
Reason for processing/collecting	The RO has requested the use of this service and is legally obliged to conduct a business improvement district ballot, or has a legitimate interest in conducting a business improvement district canvass campaign.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of printing and distributing business improvement district canvass and notification of ballot letters.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, fourteen months after the completion of the job.

6 Printing and distribution of business improvement district (BID) ballot papers

Data processor	Electoral Reform Services (“ERS”)
Project	Printing and distribution of business improvement district ballots.
Description of process	The process of facilitating the Data Controller in holding a business improvement district ballot through the physical production and, where necessary, distribution of ballot papers.
Reason for processing/collecting	The RO has requested the use of this service and is legally obliged to conduct a business improvement district ballot.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of printing and distributing business improvement district ballot papers.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, fourteen months after the completion of the job.

7 Printing and distribution of consultative ballot papers

Data processor	Electoral Reform Services (“ERS”)
Project	Printing and distribution of consultative ballots.
Description of process	The process of facilitating the Data Controller in holding a consultative ballot through the physical production and, where necessary, distribution of ballot papers.
Reason for processing/collecting	The RO has requested the use of this service and has a legitimate interest in conducting a consultative ballot.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of printing and distributing consultative ballot papers.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, fourteen months after the completion of the job.

8 Receipt and scanning of postal vote signature refresh letters

Data processor	Electoral Reform Services (“ERS”)
Project	Receipt and scanning of postal vote signature refresh letters.
Description of process	The process of facilitating the Data Controller in holding an holding an absent voter signature refresh campaign through the receipt and scanning of postal vote signature refresh letters and forms.
Reason for processing/collecting	The ERO has requested the use of this service and is legally obliged to conduct an absent voter signature refresh campaign through the receipt and scanning of postal vote signature refresh letters and forms.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of receiving and scanning postal vote signature refresh letters.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, fourteen months after the completion of the job.

9 Receipt and scanning of household enquiry forms

Data processor	Electoral Reform Services (“ERS”)
Project	Receipt and scanning of household enquiry forms.
Description of process	The process of facilitating the Data Controller in canvassing their electoral area through the receipt and scanning of household enquiry forms.
Reason for processing/collecting	The ERO has requested the use of this service and is legally obliged to conduct a canvass of their electoral area through the receipt and scanning of household enquiry forms.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of receiving and scanning household enquiry forms.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, fourteen months after the completion of the job.

10 Receipt and processing of business improvement district canvass letters

Data processor	Electoral Reform Services (“ERS”)
Project	Receiving and processing business improvement district canvass letters.
Description of process	The process of facilitating the Data Controller in holding a business improvement district canvass campaign through the receipt and processing of business improvement district canvass letters.
Reason for processing/collecting	The RO has requested the use of this service and has a legitimate interest in conducting a business improvement district canvass campaign.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of receiving and processing business improvement district canvass letters.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, fourteen months after the completion of the job.

11 Receipt, scanning and result declaration of business improvement district ballot papers

Data processor	Electoral Reform Services (“ERS”)
Project	Receiving, scanning and declaring the result for business improvement district ballot papers.
Description of process	The process of facilitating the Data Controller in holding a business improvement district ballot through the receipt, scanning and result declaration of a given ballot.
Reason for processing/collecting	The RO has requested the use of this service and is legally obliged to conduct a business improvement district ballot.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of receiving, scanning and declaring the result for business improvement district ballots.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, fourteen months after the completion of the job.

12 Receipt, scanning and result declaration of consultative ballots

Data processor	Electoral Reform Services (“ERS”)
Project	Receiving, scanning and declaring the result for consultative ballots.
Description of process	The process of facilitating the Data Controller in holding a consultative ballot through the receipt, scanning and result declaration of a given ballot.
Reason for processing/collecting	The RO has requested the use of this service and has a legitimate interest in conducting a consultative ballot.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of receiving, scanning and declaring the result for consultative ballots.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, fourteen months after the completion of the job.

13 Automated Household Response (AHR) service

Data processor	Electoral Reform Services (“ERS”)
Project	Receipt of online, telephone and Short Message Service (SMS) household responses, online distribution, online publication and the subsequent updating of household elector records.
Description of process	The process of facilitating the Data Controller in the receipt of online responses, telephone calls and Short Message Service (SMS) communication and the online distribution, online publication and subsequent update of household elector records.
Reason for processing/collecting	The RO has requested the use of this service and has a legitimate interest in both optimising the response rate and offering household electors diverse response methods for the canvass project (see Printing and distribution of forms and letters relating to electoral registration).
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of receiving online responses, telephone calls and Short Message Service (SMS) communication and the online distribution, online publication and subsequent updating of household elector records.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, fourteen months after the completion of the job.

14 Mobile Canvasser Application (MCA)

Data processor	Xpress Software Solutions Ltd (“XSSL”)
Project	Providing the Mobile Canvasser Application (MCA) service.
Description of process	The digital process of canvassing households that have not responded to a Household Enquiry Forms or individuals who have not responded to an Invitation To Register sent by the Data Controller.
Reason for processing/collecting	The ERO has requested the use of this service and is legally obliged to conduct a personal canvass of non-responding households/individuals.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of canvassing households that have not responded to a Household Enquiry Forms or individuals who have not responded to an Invitation To Register sent by the Data Controller.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, for the period from notification a personal canvass is required until two months after the completion of the personal canvass.

15 Mobile Election Application (MEA) election staff self-service

Data processor	Xpress Software Solutions Ltd (“XSSL”)
Project	Providing the Mobile Election Application (MEA) election staff self-service.
Description of process	The digital process for election staff to self-serve their employment details.
Reason for processing/collecting	The RO has requested the use of this service and has a legitimate interest in doing so.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of self-serving election staff their employment details.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, for the period from creation of the account by the RO until such time as either the member of staff is no longer employed or the RO ceases to use the Mobile Election Application service.

16 Mobile Election Application (MEA) polling places service

Data processor	Xpress Software Solutions Ltd (“XSSL”)
Project	Providing the Mobile Election Application (MEA) polling place service.
Description of process	The provision of a digital process so that those who are responsible for the booking, opening and/or closing of polling places can self-serve their details.
Reason for processing/collecting	The RO has requested the use of this service and has a legitimate interest in doing so.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of self-serving polling details.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, for the period from creation of the account by the RO until such time as either the polling place is no longer used or the RO ceases to use the Mobile Election Application service.

17 Mobile Election Application (MEA) polling station service

Data processor	Xpress Software Solutions Ltd (“XSSL”)
Project	Providing the Mobile Election Application (MEA) polling station service.
Description of process	The digital process for polling place staff to collect information.
Reason for processing/collecting	The RO has requested the use of this service and has a legitimate interest in doing so.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose of allowing polling place staff to collect information digitally.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, for the period from creation by the polling staff until such time as it’s download by the RO.

18 Data Conversions

Data processor	Xpress Software Solutions Ltd (" XSSL ")
Project	Data Conversion
Description of process	A process to convert data from one format into a format that is suitable for use with the Xpress electoral management system.
Reason for processing/collecting	The ERO/RO has requested the use of this service and has a legitimate interest in doing so.
Data Controller instructions	The Data Controller(s) instructs the Data Processor(s) to process Personal Data for the purpose converting data from one format into a format suitable for use with the Xpress systems
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project or, if no instruction has been received, for the period from notification of supply until twelve months after completion of system installation.

19 Modern.Gov Hosting

Data processor	Modern Mindset Limited (“ MML ”)
Project	Modern.Gov Hosting
Description of process	The hosting of computer systems and digital data.
Reason for processing/collecting	The Data Controller instructs the Data Processor(s) to process Personal Data for the purposes of utilising Modern.Gov meeting management software.
Data Controller instructions	The Data Controller has requested the use of this service and has a legitimate interest in doing so.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project, or upon instruction from the Data Controller at a later date.

20 Modern.Gov Support and Maintenance

Data processor	Modern Mindset Limited (“ MML ”)
Project	Modern.Gov Support and Maintenance
Description of process	Accessing and processing data held in Modern.Gov meeting management software.
Reason for processing/collecting	The Data Controller instructs the Data Processor(s) to process Personal Data for the purpose of support and maintenance of the Modern.Gov meeting management software.
Data Controller instructions	The Data Controller has requested the use of this service and has a legitimate interest in doing so.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project, or upon instruction from the Data Controller at a later date.

21 Modern.Gov Data Transfer

Data processor	Modern Mindset Limited (“ MML ”)
Project	Modern.Gov Data Transfer
Description of process	The transfer of data from the Data Controller to the Data Processor.
Reason for processing/collecting	The Data Controller instructs the Data Processor(s) to process Personal Data for the purpose of Data Transfer relating to Modern.Gov meeting management software.
Data Controller instructions	The Data Controller has requested the use of this service and has a legitimate interest in doing so.
Disposal of Personal Data	The Personal Data will be disposed of in accordance with the instructions of the Data Controller at the commencement of the project, or upon instruction from the Data Controller at a later date, in accordance with our Migration & Hosting Move Data Transfer Procedure.

SCHEDULE 6: PERSONAL DATA

The Data Controller(s) (see **SCHEDULE 3: DATA CONTROLLER(S)**) instruct The Data Processor (see **SCHEDULE 4: DATA PROCESSOR(S)**) to process Personal Data on their behalf for the sole purpose of delivering the relevant projects (see **SCHEDULE 5: PROJECTS**), as required by individual Project Specifications. The Personal Data required to deliver these projects may include the storage and processing of the following Personal Data categories:

1 For Electors:

Names
Salutations
Genders
Signatures
Dates of birth
Nationalities
National Insurance numbers
Addresses
Email addresses
IP addresses
Telephone numbers
Voting areas
Voting preferences
Opt out statuses
Evidence required to register
Numerical identifiers
Security codes

2 Polling Station Incident Data Subjects:

Data Subject names
Data Subject addresses
Incident details

3 For Ratepayers:

Ratepayer names
Ratepayer salutations
Ratepayer genders
Ratepayer signatures
Addresses
Email addresses
Telephone numbers
Numerical identifiers
Rateable values
Evidence required for identification

4 For Data Controllers:

RO names
RO contact details
ERO names
ERO contact details

5 For Staff:

Names
Salutations
Genders
Signatures
Dates of birth
Nationalities
National Insurance numbers
Addresses
Email addresses
Telephone numbers
Bank details
Invoice names
Usernames
Passwords
GPS locations
Work eligibility evidence
Driving license details
Disability statuses
Employer information
Miscellaneous notes

6 For Modern.Gov Users:

Names
Salutations
Genders
Dates of birth
Ethnicities
Religious affiliations
Marital statuses
Disability statuses
Political affiliations
Addresses
Email addresses
IP addresses
Telephone numbers
Usernames
Passwords
Interests (personal and pecuniary)
Miscellaneous notes
Configurable fields for custom user information, such as social media accounts
Documents (including restricted papers), referencing Data Subjects, taken from any combination of Boards, Hearings, Meetings, Committees, Applications, etc.

SCHEDULE 7: SUB-CONTRACTORS

The Data Processor(s) (see **SCHEDULE 4: DATA PROCESSOR(S)**), having been instructed by The Data Controller(s) (see **SCHEDULE 3: DATA CONTROLLER(S)**) to process Personal Data on their behalf for the sole purpose of delivering the relevant projects (see **SCHEDULE 5: PROJECTS**), may, for the purposes of Business Continuity, sub-contract the printing, filling, finishing and distribution of physically printed materials to its approved sub-contractors. The details of the approved sub-contractors are as follows:

"Sub-Contractor(s)"	Registered Office	Registered Number
First Move Marketing Services Limited (" FM ")	4 Fairview Estate, Kings Road, High Wycombe, HP11 1SA.	02455144
DSI Billing Service Limited (" DSI ")	Evolution House, Choats Road, Dagenham, Essex, RM9 6BF.	03823171
Hanson Direct Mail Limited (" HDM ")	3a Standard Industrial Estate, Henley Road, London, E16 2ES	03875954