Intermediary Data Protection

This document sets out the terms and conditions for data protection under the General Data Protection Regulation between you [the Intermediary] and Vernon Building Society [the Society].

1. DEFINITIONS

In this document, the following definitions apply:

"**Adequate Jurisdiction**"	means a jurisdiction outside the European Economic Area that has been determined to have in place adequate protections for personal data including under the Data Protection Laws, pursuant to a valid decision notice issued by the European Commission.
"Authorised Sub-Processor"	any third party appointed by the Intermediary with the prior written consent of the Society, to Personal Data.
"Data Protection Laws"	all applicable laws (including decisions) and guidance by relevant supervisory authorities relating to data protection, the processing of personal data and privacy, including: (a) the Data Protection Act 1998; (b) (with effect from 25 May 2018) the General Data Protection Regulation (EU) 2016/679; (c) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and (d) any legislation that, in respect of the United Kingdom, replaces or converts into domestic law the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union; and references to **"Data Controller"**, **"Data Subject"**, **"Personal Data"**, **"Process"**, **"Processed"**, **"Processing"**, **"Data Processor"** and **"Personal Data Breach"** have the meaning given to those terms in the Data Protection Laws.
"Standard Contractual Clauses"	means the EU standard contractual clauses for data processors established in third countries pursuant to European Commission Decision (2010/87/EU) of 5 February 2010 under the EU Directive (95/46/EC), or such

	other European Commission decision under the Data Protection Laws as may replace that European Commission Decision from time to time, in each case in unamended form.
"Supervisory Authority" such	means the Information Commissioner's Office or other supervisory authority as may be responsible for enforcing compliance with the Data Protection Laws from time to time.

2. DATA PROTECTION

2.1 Each party warrants that they will each duly observe all their obligations under the Data Protection Laws

2.2 The Intermediary will disclose personal data to the Society and will process personal data on behalf of the Society in order for the Society to process mortgage applications for customers. The Society and Intermediary will each act as controllers in respect of the personal data.

2.3 To the extent that the Society and Intermediary act as joint controllers in respect of the personal data, each party will be responsible for the security and the compliant transfer of the personal data it holds.

2.4 The both the Society and Intermediary will be responsible for lawfulness, fairness and accuracy, purpose limitation and compliance with the rights of the data subject.

2.5 The processing, type and categories of personal data is strictly limited to what is required for the Intermediary to provide the services, responsibilities, processes and/or functions that it is required to provide and may include, but not be limited to, customer and employee data.

2.6 The Intermediary shall in relation to personal data which the Intermediary has collected and subsequently transferred to the Society, ensure that all fair processing notices have been given (and/or, as applicable, consents obtained) and are sufficient in scope to enable the Society to process the personal data as required in order to obtain the benefit of its rights, and to fulfil its obligations in accordance with the GDPR.

2.7 Each party shall:

2.7.1 comply with the GDPR in the performance of its obligations;

2.7.2 notify the other party of any actual, suspected or 'near miss' personal data breach which may have occurred in connection with its arrangements with the Society as soon as reasonably practicable (and in any event, within twenty-four (24) hours) upon becoming aware of the same;

2.7.3 take the appropriate technical and organisational security measures to ensure the security of personal data processing in accordance with Article 32 of the GDPR.

2.8 To the extent that a party (the "processing party") acts as a processor on behalf of the other party (the "controlling party"), then in addition to the foregoing obligations it shall:

2.8.1 act only on the written instructions of the controlling party;

2.8.2 ensure that anyone processing personal data (including the processing party's individual employees and contractors) is subject to confidentiality obligations as set out within the GDPR;

2.8.3 only engage sub-processors with the prior written consent of the controlling party and under a written agreement with the sub-processor which includes data protection obligations that are no less onerous than those set out in the GDPR;

2.8.4 assist the controlling party in providing subject access and allowing data subjects to exercise their rights under Chapter III of the GDPR;

2.8.5 assist the controlling party in meeting its obligations under Articles 32 to 36 of the GDPR with regard to the security of processing, the notification of personal data breaches and data protection impact assessments;

2.8.6 delete or return all personal data to the controlling party as requested at the end of the arrangementtom unless it is required to retain the personal data by law;

2.8.7 provide the controlling party with all information that is reasonably required to show that both the controlling party and the processing party have met the obligations of this supplemental letter;

2.8.8 submit and contribute to audits and inspections carried out by the controlling party or an auditor appointed by the controlling party; and

2.8.9 inform the controlling party immediately in writing if it believes that it has been given an instruction that would infringe the GDPR or other relevant data protection legislation.