THE FOLLOWING TERMS ARE APPLICABLE TO SERVICES PROVIDED UNDER THE GO-AHEAD SHORT FORM SERVICES CONTRACT UNTIL REPLACED OR UPDATED

Notwithstanding anything else contained within this Agreement the Supplier:

1) has, and shall maintain throughout the Term, processes in place to ensure that the Services are free from malware and defects which could adversely affect the security of the Services provided to the Customer and/or any data belonging to the Customer that the Supplier stores or processes in relation to the provision of the Services (including but not limited to Personal Data) ("**Data**").

2) shall ensure that throughout the Term and thereafter for as long as any Data continues to be stored it has and maintains at least one of the following standards of certifications:

   a. Cyber Essentials (About Cyber Essentials - NCSC.GOV.UK),
   b. Cyber essentials plus,
   c. ISO22301, or
   d. ISO27001

3) shall maintain appropriate systems security in respect of the Services in accordance with Good Industry Practice such practice being, inter alia, to protect all Data and information provided by or provided by or generated by the Services on behalf of the Customer. This shall include but not be limited to ensuring all Data transported by portable storage media or by telecommunications network shall be fully encrypted or password protected / sent by secure a virtual private network as appropriate and all such data must be wiped from the storage media used for transporting the data or destroyed such that it cannot be recovered once the data has been transferred to the target system;

4) shall conduct security testing of the information technology systems used to provide the Services (including but not limited to penetration testing and vulnerability scans) at least once in each Contract Year during the Term and shall provide a copy of the results of such testing to the Customer promptly upon completion;

5) ensure that all personnel involved in the provision of the Services undergo regular information security training and are made aware of, and act in accordance with, the obligations under the Customer's Information Security policy when accessing Customer systems and these Information Security Terms with regard to the security and protection of Data;

6) shall be responsible for the security of all systems which connect to Customer systems and ensure user access is based on the principle of least privilege;

7) shall respond promptly to any questions, enquiries or questionnaires issued by the Customer regarding the Supplier's general approach to, and handling of Information Security and Data Protection issues and/or the Supplier's compliance with the Relevant Legislation and Good Industry Practice standards in relation to the same;

8) agrees that the Customer (and/ or its representatives, including its appointed auditors) may conduct an inspection or audit during normal business hours on Business Days (and subject to a minimum of five Business Days prior written notice) in order to ascertain compliance with the terms of this Agreement and these Information Security Terms, Save in the event of fraud, unlawful activity, security incident, breach or requests from a regulatory authority, such audit will be limited to once in each Contract Year. the Supplier will co-operate and respond to reasonable requests for information. Each party shall bear their own costs;;

9) shall notify the Customer promptly and in any event within 24 hours of first becoming aware of any actual, suspected or threatened information security incidents which have impacted, or which may have the potential to impact, the running of the Service, or will affect the confidentiality, integrity or

availability of the Customer's Data stored or transmitted by the Supplier. The Supplier will work with the security investigation team following any such security information incident;

10) grants the Customer the right to perform periodic vulnerability scans of websites provisioned specifically for the Customer as a tenant to check for vulnerabilities; and

11) shall, immediately following the termination of the Services and/or this Agreement securely delete or, at the Customer's request, return in a secure electronic format, all Data and inform the Customer that it has done so.

12) If the Supplier stores, processes or transmits Cardholder Data (which for the purposes of this clause shall include Primary Account Number, Cardholder Name, Expiration Date and Service Code and Sensitive Authentication Data including full track data, magnetic-stripe data or equivalent on a chip), CAV2/CVC2/CVV2/CID and PINs/PIN blocks), or has the ability to control or impact the security of Go-Ahead Cardholder Data, the Supplier warrants and undertakes that it will:

    (a) provide to the Customer a copy of its current Attestation of Compliance within 30 days of the date of this Agreement, and immediately after it renews (or obtains) its Attestation for the duration of this Agreement; and

    (b) notify Go-Ahead in the most expedient time possible under the circumstances and without unreasonable delay if at any time the Supplier becomes aware that it is no longer PCI compliant, and must, if so required by the Customer, immediately cease to process MERCHANT Cardholder Data;

    (c) comply with the Payment Card Industry Data Security Standard in respect of the MERCHANT Cardholder Data;

    (d) notify the Customer in the most expedient time possible under the circumstances and without unreasonable delay upon suspecting and/or discovering that Customer Cardholder Data was, or is reasonably believed to have been, acquired or accessed by an unauthorised person; and

    (e) be responsible for compliance with any agreed specific control objectives to maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes or transmits the customer's cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of a customer.

    (f) PCI controls performed by the Supplier will be agreed with the Customer and provided in a responsibilities' matrix to the Customer