

Dated 20th April 2018

PAYMASTER (1836) LIMITED

AND

HSC PENSION SCHEME

---

ADDENDUM TO  
THE AGREEMENT FOR INTERNATIONAL PAYMENT SERVICES DATED 16th September 2009

---

This Addendum is dated April 20 18

Between

- (1) Paymaster (1836) Limited (Registered Number 3249700) whose registered office is at Sutherland House, Russell Way, Crawley, West Sussex, RH10 1UH (Equiniti) and
- (2) HSC Pension Scheme, Waterside House, Derry, BT47 6FP (Customer),

shall amend the Agreement for the Provision of international payment services dated 16th September 2009 and subsequent amendments (the Agreement).

This Addendum supplements the Agreement and all of the terms and conditions of the Agreement apply to this Addendum provided that, to the extent there is a conflict between this Addendum and the Agreement, the terms of this Addendum shall prevail. All capitalised terms not defined herein shall have the same meaning as in the Agreement.

Whereas

- (A) On 16th September 2009 Equiniti and the Customer entered into the Agreement for the provision of international payment services.
- (B) In anticipation of the application of the General Data Protection Regulation (GDPR) as of 25 May 2018, the Parties have agreed to amend the Agreement to ensure that any and all data protection provisions contained therein are replaced in their entirety with those contained herein in order to comply with the applicable legislation.
- (C) Consequently the parties now wish to enter into this Addendum in order to record the amendments to be made to the data protection provisions contained in the Agreement.

In consideration of the mutual promises contained in this Addendum and the Agreement it is agreed as follows:

## 1 Definitions

Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement including this Addendum.

## 2 Effective date

With effect from the date of this Addendum, the Agreement shall be amended as set out in this Addendum.

### 3 Changes to the Agreement

Any and all references to Data Protection contained within the Agreement will be deleted and replaced in their entirety with the Schedule set out in Appendix A to this Addendum

### 4 Counterparts

This Addendum may be entered into by the Parties in any number of counterparts. Each counterpart shall, when executed and delivered, be regarded as an original, and all the counterparts shall together constitute one and the same instrument.

### 5 Governing Law

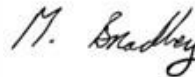
This Addendum and any non-contractual obligation arising out of or in relation to this Addendum shall be governed by and will be interpreted in accordance with English law. All disputes arising out of or relating to this Addendum or any non-contractual obligations arising out of or relating to this Addendum shall be submitted to the exclusive jurisdiction of English courts.



Signed by  
duly authorised for and on behalf of  
**Paymaster (1836) Limited**

)  
)  
)

.....  
**Operations Director, EQ Global**  
.....



Signed by  
duly authorised for and on behalf of  
**HSC Pension Scheme**

)  
)  
)

.....  
**Head of HSC Pension Service**  
.....

## Appendix A

### DATA PROTECTION SCHEDULE

#### DEFINITIONS

For the purposes of this Data Protection Schedule:

**"Affiliate"** means the Company and any other entity that, directly or indirectly through one or more intermediaries, controls, is controlled by, or is under common control of the Parties.

**"Applicable Law"** means any applicable law, legislation, bye law, regulation, order, regulatory policy (including any requirement, guidance or notice of any Regulator), guidance or industry code of practice, rule of court or directives, delegated or subordinate legislation in force from time to time and which apply to the provision of the Services;

**"Approved Sub-processor"** has the meaning provided by Appendix 2 (*Approved Sub-processors*)

**"Breach of Security"** means a breach of security caused by the Supplier or its Approved Sub-processors leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Data;

**"Business Day"** means any day other than a Saturday, Sunday or bank or other public holiday in England;

**"Change Control Procedure"** means the procedure for change or variation (as applicable) set out in the Agreement;

the terms **"Controller"**, **"Data Subject"**, **"Data Protection Impact Assessment"**, **"Personal Data"**, **"Processor"** and **"Processing"** shall have the meaning given to those terms in the GDPR, and **"Process"** and **"Processed"** shall be construed accordingly;

**"Customer"** has the same meaning as defined in the Addendum incorporating this Data Protection Schedule into the agreement dated 16th September 2009;

**"Customer Data"** means the Personal Data provided by or on behalf of the Customer pursuant to the Services for Processing by the Supplier under this Agreement;

**"Data Protection Authority"** means the Information Commissioner's Office and any other relevant Member State data protection regulator (including any successor or replacement);

**"Data Protection Laws"** means: (a) unless and until the GDPR is no longer directly applicable in the UK, the GDPR and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (b) any successor legislation in the UK to the GDPR or the Data Protection Act 1998;

**"Data Protection Losses"** means all:

- (a) costs, claims, demands, actions, expenses, losses and damages; and
- (b) to the extent permitted by Applicable Law:
  - I. administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Data Protection Authority;
  - II. compensation which is ordered by a court, tribunal or a Data Protection Authority to be paid to a Data Subject; and
  - III. the reasonable costs of compliance with investigations by a Data Protection Authority;

**"GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1, 4.5.2016 (and any successor legislation); and

**"Services"** means the services set out in the Agreement.

**"Supplier"** means Equiniti

## 1. NATURE OF THE PROCESSING AND OF THE PARTIES' RELATIONSHIP AS CONTROLLER AND PROCESSOR

1.1 Each Party shall comply with its obligations under the Data Protection Laws in relation to the Customer Data and with its obligations under this Data Protection Schedule.

1.2 Save as set out in paragraph 1.4 and 4 (Regulatory Obligations of Supplier) or as otherwise agreed in writing between the Parties, the Parties acknowledge and agree that the Customer shall act as the Controller and the Supplier shall act as the Customer's Processor in connection with the Processing by the Supplier of the Customer Data under this Agreement.

1.3 Appendix 1 to this Data Protection Schedule sets out the subject matter, duration, nature and purpose of Processing, types of Personal Data and Categories of Data Subject to be Processed under this Agreement on behalf of the Customer as data controller. The Parties may update Appendix 1 (Data Protection Particulars) from time to time by agreement in writing.

1.4 The Parties acknowledge and agree that the Supplier shall act as a Controller where the Customer Data is being Processed by the Supplier for the purposes of:

1.4.1 services contracted directly with the Data Subjects; and/or

1.4.2 the Supplier complying with its own regulatory obligations, including without limitation, as set out in paragraph 4 (Regulatory Obligations of Supplier),

and that in relation to such purposes: (i) the Supplier shall be entitled to Process the Customer Data; (ii) the obligations and restrictions set out in paragraph 2 (*The Supplier's Obligations as Processor*) shall not apply; and (iii) the Supplier may transfer Customer Data outside the European Economic Area.

## 2. THE SUPPLIER'S OBLIGATIONS AS A PROCESSOR

2.1 Subject to paragraphs 1.4 and 4 (Regulatory Obligations of Supplier), the Supplier shall:

2.1.1 only process Personal Data for and on behalf of the Customer, in accordance with the Customer's written instructions, for the sole purpose of performing the Services, and otherwise in accordance with the terms of this Data Protection Schedule. Any instruction issued by the Customer that, whilst not constituting a variation of the Agreement nevertheless has the effect of varying the Supplier's existing data processing procedures or operating model, shall be treated and processed as a change in accordance with the Change Control Procedure;

2.1.2 not transfer any Customer Data outside of the European Economic Area unless the prior consent of the Customer has been obtained and the Customer or the Supplier has provided appropriate safeguards in relation to the transfer. In relation to this paragraph 2.1.2, the Customer:

(a) shall not unreasonably withhold or delay its consent to such a transfer or its agreement to, or assistance in relation to, appropriate safeguards (including, for example, by entering into appropriate data protection model clauses);

- (b) agrees that this Agreement constitutes consent for the Supplier to transfer Customer Data to its Affiliates in the UK; and to any particular Sub-processor agreed additionally in accordance with Appendix 2 (Approved Sub-processors); and
  - (c) shall, and shall procure that any relevant third party shall, use all reasonable endeavours to provide all necessary notifications to data subjects and, where applicable, obtain all consents as may be necessary to ensure that such transfers of Customer Data are compliant with Data Protection Laws.
- 2.1.3 ensure that persons authorised to process the Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- 2.1.4 maintain the technical and organisational security measures in accordance with the Supplier's Information Security Schedule as set out in Appendix 3. The Customer acknowledges and agrees that such technical and organisational security measures are appropriate to protect the Customer Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of processing, including where the processing involves the transmission of data over a network;
- 2.1.5 not disclose or allow access to Customer Data to a third party (including to a sub-processor) except to an Approved Sub-processor or in accordance with Appendix 2 (Approved Sub-processors) or otherwise as permitted under the Agreement;
- 2.1.6 subject to paragraph 2.3, assist the Customer (when reasonably requested to do so and provided that the request is made promptly and includes all information reasonably necessary to action the request):
  - (a) to comply with any request or notice from a Data Subject exercising their rights under the Data Protection Laws in relation to the Customer Data or any communication from the Data Protection Authority in relation to the Processing of the Customer Data by the Supplier under this Agreement; and
  - (b) in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, notifying a Data Protection Authority or a Data Subject of a Breach of Security and where the Customer decides to carry out a Data Protection Impact Assessment (including any resulting consultation with the Data Protection Authority),  
  
in each case insofar as this is possible and taking into account the nature of the Processing and the information available to the Supplier.
- 2.1.7 at the Customer's option or direction on termination or expiry of the Agreement, arrange within a reasonable time period for the return and/or deletion of all Customer Data or for its encryption or anonymisation so as to render the Data Subject's identification impossible, or for the Customer Data otherwise to be put beyond use. Notwithstanding the foregoing, for the avoidance of doubt the Supplier may retain Customer Data where (i) 1.4 applies and/or where (ii) this is necessary for the purpose

of defending itself or its Affiliates in relation to any claim or legal proceedings; and/or where (iii) it is required by Applicable law to keep copies of the Customer Data;

- 2.1.8 inform the Customer immediately if it considers in its opinion that any of the Customer's instructions infringe Data Protection laws. Nothing in any instructions issued by or on behalf of the Customer under this Agreement shall require the Supplier to infringe any Data Protection laws, and the Supplier shall not be in breach of its instructions or its obligations under this Agreement by failing to observe any such instructions; and
  - 2.1.9 where a Breach of Security occurs of which the Supplier becomes aware, in relation to Customer Data under or in connection with this Agreement, notify the Customer without undue delay after becoming aware.
- 2.2 Subject to paragraphs 2.2.4 and 2.3, the Supplier shall make available to the Customer all information relevant to this Agreement which is necessary to demonstrate its compliance with the obligations laid out within Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer, provided that:
- 2.2.1 the first audit or inspection in any 12 month period shall be at no cost to the Customer. For any additional audit or inspection in the same 12 month period, the Supplier shall be entitled to charge the Customer a reasonable fee in accordance with paragraph 2.3 below;
  - 2.2.2 the parties agree that the Supplier may, where so requested by the Customer, meet its audit obligations to the Customer by providing the Customer with a report of its compliance with its data protection obligations based on the American Institute of Certified Public Accountants under the Service Organization Controls (SOC) framework 2 type II standard;
  - 2.2.3 nothing in this Agreement shall prohibit the Customer from seeking an additional audit or inspection where in its reasonable opinion the said report does not address all of the data protection compliance matters that the Customer wishes to audit, subject to payment by the Customer of the Supplier's charges in accordance with paragraph 2.3; and
  - 2.2.4 any audit or inspection must be conducted during normal business hours on a Business Day and on the provision of reasonable advance notice to the Supplier. The Customer shall use its reasonable endeavours to ensure that the conduct of such audit does not unreasonably disrupt the business of the Supplier. The Customer undertakes to keep all information obtained strictly confidential and where an agent or representative of the Customer is authorised to conduct an audit on behalf of the Customer it shall undertake in advance to the Supplier to keep all information obtained strictly confidential and not to use or disclose any such information except for the purpose of reporting the results of its audit to the Customer.
- 2.3 The Supplier shall be entitled to charge a reasonable fee (calculated on a time and materials basis at the rates agreed by the Parties from time to time or in accordance with any rate cards), or as otherwise agreed by the parties for:



- 2.3.1 the assistance set out in paragraph 2.16;
- 2.3.2 work undertaken in relation to any additional audit under paragraphs 2.2.1 and 2.2.3; and/or
- 2.3.3 any work undertaken to implement and comply on an ongoing basis with: (a) any changes to Data Protection Laws (including as a result of a withdrawal of the United Kingdom from the European Union); (b) any changes to the security measures taken by the Supplier in respect of the Services in order to maintain compliance with the Data Protection Legislation; and/or (c) any order, direction or instruction of the Data Protection Authority in respect of the Supplier's performance of the Services.

### 3. THE CUSTOMER'S OBLIGATIONS AS CONTROLLER

#### 3.1 The Customer represents, warrants and undertakes:

- 3.1.1 that the Customer's instructions to the Supplier in connection with or arising out of the Processing of the Customer Data on the Customer's behalf are and will at all times be lawful and shall not contravene any Data Protection Laws;
- 3.1.2 that the Processing of Customer Data by or on behalf of the Customer (up to and including the making available of the Customer Data to the Supplier) has been and will continue at all times to be carried out in accordance with the relevant provisions of the Data Protection Laws (and, where applicable, has been notified to the relevant authorities of the Member State where the Customer is established) and does not contravene any Data Protection Laws;
- 3.1.3 that the Processing by the Supplier, in accordance with and as contemplated by this Agreement will not contravene any Data Protection Laws;
- 3.1.4 without limiting the generality of the foregoing, (save where the Supplier is the Controller), that the Customer has and will continue at all times to have in place all fair processing notices and (where applicable) consent mechanisms for Data Subjects sufficient to ensure that all Processing of Customer Data by the Supplier, in accordance with this Data Protection Schedule, that is contemplated by this Agreement, will be lawful and shall not contravene any Data Protection Laws; and
- 3.1.5 that the Customer will incorporate the processing carried out by the supplier as set out in Appendix 1 into the Customer's fair processing notices (including without limitation those referred to in paragraph 3.1.4)..

#### 3.2 The Customer shall, at the Supplier's written request, provide the Supplier with reasonable evidence that it has in place all necessary fair processing notices (including the Supplier's Processing as set out in Appendix 1) and consents required for the processing of Customer Data.

### 4. REGULATORY OBLIGATIONS OF SUPPLIER

#### 4.1 Notwithstanding any other provision of this Agreement, the Supplier shall be entitled to respond to regulators which regulate the Supplier and take any other actions as necessary to deal with any orders, demands, correspondence, requests for information or other similar matters relating

to the performance by the Supplier of its regulatory obligations under or in connection with this Data Protection Schedule. The Parties acknowledge and agree that the Supplier shall act as a Controller where the Customer Data is being Processed for this purpose and that the Supplier may transfer Customer Data outside the European Economic Area for this purpose.

- 4.2 Where the Supplier is subject to a requirement of English law or European Union Law or the law of one of the other countries of the European Union which may conflict with or be inconsistent with its obligations under this Data Protection Schedule, compliance with such a requirement will not be in breach of its obligations in this Data Protection Schedule. The Supplier shall, to the extent legally permissible, inform the Customer if the Supplier is subject to such a requirement or is made subject to one.

## 5. LIABILITY

- 5.1 The Supplier acting as Processor shall, subject to the limitation of liability in paragraph 5.3, indemnify and keep indemnified the Customer in respect of all Data Protection Losses suffered or incurred by, awarded against or agreed to be paid by, the Customer arising from or in connection with any non-compliance by the Supplier with the Data Protection Laws.
- 5.2 The Customer acting as Controller, shall, subject to the limitation of liability in paragraph 5.3, indemnify and keep indemnified the Supplier in respect of all Data Protection Losses suffered or incurred by, awarded against or agreed to be paid by, the Supplier and any Approved Sub-processor arising from or in connection with any non-compliance by the Customer with the Data Protection Laws;
- 5.3 Each party's aggregate liability to the other in respect of all claims arising out of or in connection with this Data Protection Schedule (including without limitation as a result of breach of this Data Protection Schedule, negligence or any other tort, under statute, indemnity or otherwise) will be limited to 100% of the transaction fees collected under the Agreement in the last 12 months. The liability cap set out in this paragraph operates as a separate, stand-alone, liability cap in respect of each party's liability and shall not be subject to any other liability cap(s) set out in this Agreement.

## 6. NOTICE

- 6.1 Notwithstanding any notice provisions contained within the Agreement to the contrary, any notice given by the Supplier to the Customer under this Data Protection Schedule shall be by email and shall be deemed delivered on receipt of a read receipt email from the address set out in paragraph 6.2.
- 6.2 The Customer's email address for service of notice by the Supplier to the Customer under this Data Protection Schedule is: [hscpensions@hscni.net](mailto:hscpensions@hscni.net)
- 6.3 This paragraph does not apply to notice given in legal proceedings, arbitration or other dispute resolution proceedings.

## APPENDIX 1

### International Payment Services

<p>The subject matter and duration of the Processing</p>	<p><b>SUBJECT MATTER:</b> Payment of UK based pensions into overseas jurisdictions as requested by the Pension Scheme Trustees and on receipt of Beneficiary signed instructions.</p> <p><b>DURATION OF PROCESSING:</b> Data relating to the payment of overseas pensions, including the administration and management of Pension Scheme Trustees' data subject records on a minimum 3 year, endless contract, unless terminated by either party.</p> <p>For the duration of the Agreement or in accordance with instructions from the Customer or for the duration required by legislation.</p>
<p>The nature and purpose of the Processing</p>	<p><b>PURPOSES OF PROCESSING :</b> Storage, retrieval and other support as necessary in relation to the payment of money to individuals living outside the UK on behalf of pension scheme trustees and corporate clients' pension services.</p> <p><b>LEGAL BASIS FOR PROCESSING:</b> This must be determined by the relevant controller from the list in Article 6 GDPR. The controller should include this in the contract.</p> <p><b>NATURE OF PROCESSING:</b> To manage and operate data subject accounts with EQ Paymaster to facilitate the provision of services, this includes retaining records of data subject instructions and telephone calls and keeping data subject account records up to date.</p> <p>To notify Pension Scheme Trustees &amp; corporate clients' pension services about changes to our service and to send data subject service emails relating to data subject account.</p>
<p>The type of Personal Data being Processed</p>	<p><b>PERSONAL DATA:</b> Includes but is not restricted to an individual's name, postal address, email address, phone number and financial information required to deliver payments overseas.</p> <p><b>SPECIAL CATEGORIES OF PERSONAL DATA:</b> Includes where relevant to a particular case the individual's nationality and Date of Birth.</p>
<p>The categories of Data Subjects</p>	<p>Pensioners and Dependants as appropriate.</p>

## APPENDIX 2

### APPROVED SUB-PROCESSORS

#### A. APPROVED SUB-PROCESSORS

- i. A sub-processor is an "**Approved Sub-Processor**" where:
  - a. the sub-processor is agreed in writing between the Parties but does not include Equiniti Affiliates;
  - b. the Customer has agreed to the appointment of such sub-processor elsewhere under or in accordance with this Agreement (for example pursuant to an approval to appoint a sub-contractor) ; and/or
  - c. the sub-processor is appointed by the Supplier in accordance with sub-paragraph .iv below.
- ii. The Supplier undertakes to ensure that the sub-processing contract will be on terms that are substantially the same as the terms set out in paragraph 2 of this Data Protection Schedule .
- iii. The Customer agrees that this Agreement constitutes written consent to disclosure of the Customer Data to such sub-processors .
- iv. The Supplier may appoint a new sub-processor as an Approved Sub-processor, replace an existing Approved Sub-processor or alter the scope or location of the sub-processing carried out by an Approved Sub-processor (a "**sub-processing change**") provided that:
  - a. The Supplier has given the Customer written notice of the relevant sub-processing change;
  - b. having undertaken due diligence on the sub-processor with all due skill and care, including a risk assessment of the information governance related practices and processes of the sub-contractor where the outcome of the due diligence is a determination that the sub processor and the arrangements made for the sub-processing would objectively be adequate and sufficient to ensure compliance with the applicable requirements of Data Protection Laws **adequate**"), and notice of the outcome has been provided to the Customer;
  - c. the Supplier undertakes to ensure that the sub-processing contract will be on terms that are substantially the same as the terms set out in paragraphs 2.1 and 2.2 of this Data Protection Schedule; and
  - d. the Customer has not provided evidence disproving the findings of the due diligence and the Supplier's assessment of adequacy) to the use of the sub-processor within [14] days.

## APPENDIX 3

### INFORMATION SECURITY SCHEDULE

#### 1. DEFINITIONS

"Confidential Information" means any information, however conveyed or presented, that relates to the business, affairs, operations, customers, processes, budgets, pricing policies, product information, strategies, developments, trade secrets, know-how, personnel and suppliers of a party, together with all information derived by a party from any such information and any other information clearly designated by a party as being confidential to it (whether or not it is marked "confidential"), or which ought reasonably be considered to be confidential.

"Portable Media and Devices" includes, but is not limited to, USB sticks, SO cards, portable drives, CDs and DVDs.

"Staff" means any employees, officers, directors, contractors, agents or temporary personnel (which for the avoidance of doubt shall include Approved Sub-Processors, employed or engaged by the Supplier and who have access to the Supplier premises and Systems).

"Systems" means the Supplier computer networks and software applications used to perform Services.

#### 2. GENERAL

2.1 Subject to any specific information security obligations elsewhere under or in accordance with this Agreement (which shall continue to apply in full force and effect), this Information Security Schedule shall apply to the Services.

2.2 The Supplier shall ensure that an effective information security management system (as per ISO 27001 as amended) is implemented and is aligned to the requirements of ISO 27001 (or any subsequent international information security standard that replaces ISO 27001).

#### 3. HUMAN RESOURCES

3.1 The Supplier shall:

3.1.1 have processes in place to undertake appropriate screening of Staff;

3.1.2 ensure that all Staff have either a signed employment contract or contract for services (as the case may be) which shall include appropriate confidentiality and applicable security obligations; and

3.1.3 ensure that Staff undertake appropriate awareness training relevant to their work upon commencement of work and regularly thereafter .

## 4. ACCESS CONTROL

4.1 The Supplier shall ensure that:

4.1.1 the appropriate logical and physical access procedures and controls are in place to restrict access to Systems and premises to those only with a legitimate business need; and

4.1.2 access to Systems and premises is on the basis of the lowest level of privilege required to fulfil the role.

## 5. DISPOSAL/ DESTRUCTION

5.1 The Supplier shall ensure that:

5.1.1 any Confidential Information reproduced in a hard-copy format shall be physically destroyed when it is no longer needed. This may include shredding or disposal by an appropriate waste paper destruction service; and

5.1.2 Portable Media and Devices are destroyed and disposed of in a manner which ensures that any stored information is rendered unrecoverable .

## 6. CRYPTOGRAPHY

6.1 The Supplier shall:

6.1.1 ensure that any electronic Confidential Information transfers over public /non-secure network are undertaken securely using appropriate encryption methods;

6.1.2 have appropriate technical controls to prevent the unauthorised transfer of Customer Data to Portable Media and Devices; and

6.1.3 ensure that Confidential Information is not stored on Portable Media and Devices unless appropriately encrypted.

## 7. PHYSICAL AND ENVIRONMENTAL SECURITY

7.1 The Supplier shall ensure that appropriate physical and environmental procedures and controls are in place to safeguard premises and physical equipment.

## 8. OPERATIONS SECURITY

8.1 The Supplier shall:

8.1.1 at its sole discretion, implement readily available software to detect, report and remove or quarantine malicious software /code in systems in accordance with standard industry practice in relation to the Services provided;

- 8.1.2 ensure there is a process to back-up copies of Customer Data and that the procedure is tested regularly and is in accordance with the Supplier's own internal retention policies. Back-ups shall be secured through physical protection and the use of encryption; and
- 8.1.3 ensure that timely information about technical vulnerabilities of Systems used shall be obtained, any exposure to such vulnerabilities evaluated, and effective measures taken to address the associated risk.

## 9. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

- 9.1 Within the software development lifecycle, production data will not be used in testing. In the event that testing requires the use of production data, then the express permission of the Data Controller will first be obtained.

## 10. SUPPLIER RELATIONSHIPS

- 10.1 The Supplier may engage sub-contractors to provide some or all of the Services, the Supplier shall perform appropriate due diligence and impose contractual obligations on the sub-contractor that are consistent to those contained in this Schedule.

## 11. INCIDENT MANAGEMENT

- 11.1 The Supplier shall:
  - 11.1.1 put in place the necessary processes and procedures that will allow the Supplier to make all reasonable endeavours to detect any unauthorised physical access or logical access or other breaches of this Information Security Schedule.
  - 11.1.2 establish and document a 'Security Incident' response procedure, which shall encompass the identification, classification and escalation of security incident reports and the process of confirmations of resolution.
  - 11.1.3 use reasonable endeavours to notify the Customer as soon as reasonably possible of any unauthorised access or other breach of security involving Customer data.

## 12. ASSURANCE AND RIGHT TO AUDIT

- 12.1 On an annual basis, the Supplier shall provide responses to a Customer information security questionnaire for the purposes of measuring compliance with this Information Security Schedule. The Customer shall provide the questionnaire with at least 4 weeks' notice of the due date for submission or return.

Subject always to the terms of the Agreement (which shall take precedent over this clause) following reasonable notice and the mutual agreement of timing, the Customer's information security team or their nominated auditors may conduct a review of the security controls and procedures in place at the Supplier.

