SCHEDULE 2 – APPROPRIATE ORGANISATIONAL AND TECHNICAL SECURITY MEASURES

1.1 The Parties shall implement and maintain security standards, facilities, controls, and procedures appropriate to the nature of the Shared Personal Data held by it and the harm that would be caused by its loss or disclosure including a comprehensive and up-to-date data protection policy. The Parties shall ensure that all their personnel who have access to the Shared Personal Data shall comply with the obligations upon them contained in the data protection policy.

1.2 Each Party shall ensure:

a) that it has properly configured access rights for its personnel including a well-defined joiners and leavers process to ensure access rights to the Shared Personal Data are properly managed;

b) that it has proper controls in place to make sure that complex alphanumeric passwords are required for access to the Shared Personal Data and that training is provided in relation to the need to keep such passwords secure;

c) it has in place procedures to identify wrongful use of Shared Personal Data, including the monitoring of wrongful access to Shard Personal Data;

d) suitable and effective authentication processes are established and used to protect Shared Personal Data;

e) Shared Personal Data is backed up on a regular basis and that all back up data is subject to such vigorous security procedures as are necessary in order to protect data integrity, such security measures being commensurate to the nature of the data. The Parties shall take particular care when transporting backup data and other personal data and shall ensure such backup data and other personal data is transported in a safe and secure manner;

f) Shared Personal Data transferred electronically is encrypted;

g) information stored on laptops or other portable media is encrypted and that the Parties maintains an accurate, up to date asset register, including all such portable media used to process the Shared Personal Data;

h) that suitable physical security measures are established commensurate to the harm that could result from the unlawful disclosure of the Shared Personal Data. Such physical security measures shall be as identified in the Parties data protection policy;

i) without prejudice to the Parties obligations in relation to the disposal of Shared Personal Data, all Shared Personal Data which is disposed of must be disposed of pursuant to the Parties policy for the disposal of Personal Data identified in the data protection policy, including the disposal of assets containing Shared Personal Data, a copy of which policy shall be provided, on request, to the other Party; and

j) the Parties establishes and maintains adequate data security compliance policies and audits its use of Personal Data in compliance with its data security policies on a regular basis and in any event annually.