Kent Surrey Sussex
Academic Health Science
Network

Unity
Insights

EXAMPLE VERSION

DATA PROCESSING AGREEMENT (DPA)

between

(1) Add name of trust here

of

Add address here

and

(2) Kent Surrey Sussex AHSN Limited

and

(3) Unity Insights Limited

of

**Amelia House, Crescent Road, Worthing, West
Sussex, BN11 1RL**

Email: kssahsn.data@nhs.net

KSS AHSN ref: TBC
Unity Insights ref: TBC

THIS AGREEMENT is made TBC and is valid until the (insert date of multi-year agreement period) upon which it will be reviewed in line with the terms in the cover letter.

BETWEEN:

(1) **Trust name** a hospital Trust registered in England of **Address here** ("Controller") and

(2) **Kent Surrey Sussex AHSN Limited** a private company limited by guarantee without share capital registered in England and Wales under number 08877964 whose registered office is at Amelia House, Crescent Road, Worthing, West Sussex, BN11 1RL ("Processor")

(3) **Unity Insights Limited** a private company limited by guarantee without share capital registered in England and Wales under number 13537227 whose registered office is at Amelia House, Crescent Road, Worthing, West Sussex, BN11 1RL ("Processor")

WHEREAS:

(1) The Controller from time to time engages the Processor to provide to the Controller with the Services described in Schedule 1.

(2) The provision of the Services by the Processor involves it in processing the Personal Data described in Schedule 2 on behalf of the Controller.

(3) Under Article 28(3) of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), the Controller is required to put in place an agreement in writing between the Controller and any organisation which processes personal data on its behalf governing the processing of that personal data.

(4) The Parties have agreed to enter into this Agreement to ensure compliance with the said provisions of the UK GDPR in relation to all processing of the Personal Data by the Processor for the Controller.

(5) The terms of this Agreement are to apply to all processing of Personal Data carried out for the Controller by the Processor and to all Personal Data held by the Processor in relation to all such processing.

IT IS AGREED as follows:

1. Definitions and Interpretation

1.1 In this Agreement, unless the context otherwise requires, the following expressions have the following meanings:

“Commissioner” means the Information Commissioner (as defined in Article 4(A3) UK GDPR and section 114 Data Protection Act 2018;

“Controller” shall have the meanings given to the term “controller” by Article 4(7) of the UK GDPR and section 6 of the Data Protection Act 2018;

“Data Protection Legislation” means all applicable legislation in force from time to time in the United Kingdom applicable to data protection and privacy including, but not limited to, the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder); and the Privacy and Electronic Communications Regulations 2003 as amended;

“Data Subject” means an identified or identifiable living individual to whom Personal Data relates;

“Personal Data” means any information relating to an identified or identifiable living individual; an identified or identifiable living individual 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 the individual;

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed;

“Processor” means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of a Controller;

“processing”, “process”, “processed”, “processes” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

“Services” means those services and /or facilities described in Schedule 1 which are provided by the Processor to the Controller and which the Controller uses for the purposes described in Schedule 1;

“Term” the Term of this Agreement shall be from 8th of November 2021 until the 31st March 2023, where it will be reviewed; and

“UK GDPR” means Regulation (EU) 2016/679 General Data Protection Regulation as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.

1.2 Unless the context otherwise requires, each reference in this Agreement to:

a) “writing”, and any cognate expression, includes a reference to any communication effected by electronic or facsimile transmission or similar means;

b) a statute or a provision of a statute is a reference to that statute or provision as amended or re-enacted at the relevant time;

c) “this Agreement” is a reference to this Agreement and each of the Schedules as amended or supplemented at the relevant time;

d) a Schedule is a schedule to this Agreement; and

e) a Clause or paragraph is a reference to a Clause of this Agreement (other than the Schedules) or a paragraph of the relevant Schedule.

f) a "Party" or the "Parties" refer to the parties to this Agreement.

1.3 The headings used in this Agreement are for convenience only and shall have no effect upon the interpretation of this Agreement.

1.4 Words imparting the singular number shall include the plural and vice versa.

1.5 References to any gender shall include any other gender.

1.6 References to persons shall include corporations.

2. Scope and Application of this Agreement

2.1 The provisions of this Agreement shall apply to the processing of the Personal Data described in Schedule 2, carried out for the Controller by the Processor, and to all Personal Data held by the Processor in relation to all such processing, whether such Personal Data is held at the date of this Agreement or received afterwards.

2.2 Schedule 2 describes the type(s) of Personal Data, category or categories of Data Subject, the nature of the processing to be carried out, the purpose(s) of such processing, and the duration of such processing.

2.3 The provisions of this Agreement supersede any other arrangement, understanding, or agreement made between the Parties at any time relating to the Personal Data.

2.4 This Agreement shall continue in full force and effect for so long as the Processor is processing Personal Data on behalf of the Controller, and thereafter as provided in Clause 10.

3. Provision of the Services and Processing Personal Data

3.1 The Controller shall retain control of the Personal Data and shall, at all times, remain responsible for its compliance obligations under the Data Protection Legislation including, but not limited to, providing any and all required notices and obtaining any and all required consents, and for the written processing instructions given to the Processor.

3.2 The Processor shall only provide the Services and process the Personal Data received from the Controller:

a) for the purposes of those Services and not for any other purpose;

b) to the extent and in such a manner as is strictly necessary for those purposes; and

c) strictly in accordance with the express written authorisation and instructions of the Controller (which may be specific instructions or instructions of a general nature, or as otherwise notified by the Controller to the Processor).

4. Data Protection Compliance

4.1 All instructions given by the Controller to the Processor shall be made in writing and shall at all times be in compliance with the Data Protection Legislation. The Processor shall act only on such written instructions from the Controller unless the Processor is required by law to do otherwise (as per Article 29 of the UK GDPR).

4.2 The Processor shall promptly comply with any request from the Controller requiring the Processor to amend, transfer, delete, or otherwise dispose of the Personal Data, or to stop, mitigate, or remedy any unauthorised processing.

4.3 The Processor shall transfer all Personal Data to the Controller on the Controller’s request in the formats, at the times, and in compliance with, the Controller’s written instructions.

4.4 Both Parties shall comply at all times with the Data Protection Legislation and shall not perform their obligations under this Agreement or any other agreement or arrangement between them in such way as to cause either Party to breach any of its applicable obligations under the Data Protection Legislation.

4.5 The Controller hereby warrants, represents, and undertakes that the Personal Data shall comply with the Data Protection Legislation in all respects including, but not limited to, its collection, holding, and processing, and that the Controller has in place all necessary and appropriate consents and notices to enable the lawful transfer of the Personal Data to the Processor.

4.6 The Processor agrees to comply with any reasonable measures required by the Controller to ensure that its obligations under this Agreement are satisfactorily performed in accordance with the Data Protection Legislation and any best practice guidance issued by the Commissioner.

4.7 The Processor shall provide all reasonable assistance, at the Controller’s cost, to the Controller in complying with its obligations under the Data Protection Legislation with respect to the security of processing, the notification of Personal Data Breaches, the conduct of data protection impact assessments, and in dealings with the Commissioner. What is reasonable, for the purposes of this sub-Clause shall take account of the nature of the Processor’s processing and the information available to the Processor.

4.8 The Processor shall notify the Controller in a timely manner of any changes to the Data Protection Legislation that may adversely affect its performance of the Services or of its obligations under this Agreement.

4.9 When processing the Personal Data on behalf of the Controller, the Processor shall:

a) not transfer the Personal Data outside the United Kingdom without the prior written consent of the Controller;

b) not transfer any of the Personal Data to any third party without the written consent of the Controller and, in the event of such consent, the Personal Data shall be transferred strictly subject to the terms of a suitable agreement, as set out in Clause 11;

c) process the Personal Data only to the extent, and in such manner, as is necessary in order to comply with its obligations to the Controller or as may be required by law (in which case, the Processor shall inform the Controller of the legal requirement in question before processing the Personal Data for that purpose unless prohibited from doing so by law);

d) implement appropriate technical and organisational measures, including those described in Schedule 3, and take all steps necessary to protect the Personal Data against accidental, unauthorised, or unlawful processing, access, copying, modification, reproduction, display, or distribution of the Personal Data, and against its accidental or unlawful loss, destruction, alteration, disclosure, or damage. The Processor shall inform the Controller in advance of any changes to such measures;

e) implement measures to ensure a level of security proportionate to the risks involved including, as appropriate:

   i) the pseudonymisation and encryption of Personal Data;

   ii) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;

   iii) the ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident; and

   iv) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

f) if so requested by the Controller (and within the timescales required by the Controller) supply further details of the technical and organisational systems in place to safeguard the security of the Personal Data held and to prevent unauthorised access;

g) keep complete and accurate records and information concerning all processing activities carried out on the Personal Data in order to demonstrate its compliance with this Agreement and the Data Protection Legislation;

h) make available to the Controller any and all such information as is reasonably required and necessary to demonstrate the Processor's compliance with the Data Protection Legislation;

i) on reasonable prior notice, submit to audits and inspections and provide the Controller with any information reasonably required in order to assess and verify compliance with the provisions of this Agreement and both Parties' compliance with the requirements of the Data Protection Legislation. The requirement to give notice will not apply if the Controller believes that the Processor is in breach of any of its obligations under this Agreement or under the law; and

j) inform the Controller immediately if it is asked to do anything that infringes the Data Protection Legislation.

5. Data Subject Requests, Notices, Complaints, and Personal Data Breaches

5.1 The Processor shall at the Controller's cost, assist the Controller in complying with its obligations under the Data Protection Legislation. In particular, the provisions of this Clause 5 shall apply to requests by Data Subjects to exercise their rights including, but not limited to, subject access requests, information or assessment notices served on the Controller by the Commissioner under the Data Protection Legislation, complaints, and Personal Data Breaches.

5.2 The Processor shall notify the Controller immediately in writing if it receives:

a) a request from a Data Subject to exercise their rights; or

b) any other complaint, notice, communication, or request relating to the processing of the Personal Data or to either Party's compliance with the Data Protection Legislation.

5.3 The Processor shall, at the Controller's cost, cooperate fully with the Controller and assist as required in relation to any Data Subject request, or other complaint, notice, communication, or request, including by:

a) providing the Controller with full details of the complaint, notice, communication, or request;

b) providing the necessary information and assistance in order to comply with a request from a Data Subject;

c) providing the Controller with any Personal Data it holds in relation to a Data Subject (within the timescales required by the Controller); and

d) providing the Controller with any other information requested by the Controller.

5.4 The Processor shall not disclose any Personal Data to any Data Subject or to any other third party unless instructed to do so by the Controller in writing, or as required by law.

5.5 The Processor shall notify the Controller immediately if it becomes aware of any form of Personal Data Breach, including any unauthorised or unlawful processing, loss of, unintended damage to, or destruction of any of the Personal Data.

5.6 If an event of the type described under sub-Clause 5.5 occurs:

a) Where recovery of the affected Personal Data is possible, the Processor shall recover the same as soon as possible at its own expense.

b) The Processor shall, without undue delay and at its own expense, also provide the following information to the Controller:

i) a description of the nature of the event, including the category or categories of Personal Data affected, the approximate number of Personal Data records and Data Subjects involved;

ii) the likely consequences of the event; and

iii) a description of the measures that have been taken or will be taken in response, including those to mitigate potential adverse effects.

c) The Processor shall provide, at its own expense, all reasonable co-ordination, co-operation, and assistance to the Controller in the Controller's investigation and handling of the event.

d) The Processor shall not inform any third parties of the event without the Controller's express written consent, unless required to do so by law.

e) The Controller shall have the sole right to determine whether to provide notice of the event to any Data Subjects, the Commissioner, other applicable regulators, law enforcement authorities, or other parties, as required by law or regulation or at the Controller's discretion.

f) The Controller shall have the sole right to determine whether to offer any form of remedy to affected Data Subjects.

g) Where the Processor is required to take action and/or provide assistance at its own expense under this sub-Clause 5.6, the requirement for the Processor to cover such expenses shall not apply if the event arose from the Controller's specific written instructions, negligence, wilful default, or breach of this Agreement. In such cases, the Controller shall cover all such reasonable expenses.

h) The Processor shall, in addition to taking the abovementioned actions and/or providing the abovementioned assistance at its own expense, reimburse the Controller for reasonable expenses incurred by the Controller when responding to the event, including the costs of any notices and remedies.

6. Staff and Data Protection Officers

6.1 The Processor shall ensure that all personnel who are to access and/or process any of the Personal Data:

a) be informed of the confidential nature of the Personal Data and be bound by contractual use restrictions and confidentiality requirements, as per sub-Clause 10.2;

b) be given appropriate training on the Data Protection Legislation and how their job roles relate to it and are affected by it; and

c) be made aware of both the Processor's duties, and their personal duties and obligations under the Data Protection Legislation and this Agreement.

6.2 [The Controller has appointed a data protection officer in accordance with Article 37 of the UK GDPR, whose details are as follows: **Add DPO name, Trust name, and address**

6.3 The Processor has appointed a data protection officer in accordance with Article 37 of the UK GDPR, whose details are as follows:
Nick Birch, Exigia Ltd., Kemp House, 152-160 City Road, London EC2V 1NX.

7. Warranties

7.1 The Processor warrants and represents that:

a) its employees, subcontractors, agents, and any other person or persons accessing and otherwise handling the Personal Data on its behalf are appropriately trained with respect to compliance with the Data Protection Legislation;

b) it, and any party acting on its behalf, will process the Personal Data in compliance with the Data Protection Legislation and any and all other applicable laws, regulations, standards, and similar instruments;

c) nothing, in its reasonable belief, in the Data Protection Legislation prevents it from providing the Services;

d) it will take all appropriate and proportionate technical and organisational measures to prevent the accidental, unauthorised, or unlawful processing of the Personal Data and the loss of or damage to the Personal Data, ensuring a level of security appropriate in light of:

i) the potential harm resulting from such an event;

ii) the nature of the Personal Data in question;

iii) the measures necessary to comply with all applicable Data Protection Legislation and all relevant policies and procedures.

7.2 The Controller warrants and represents that the Processor's use of the Personal Data in its provision of the Services and as specifically instructed by the Controller shall comply with the Data Protection Legislation.

8. Liability and Indemnity

8.1 The Controller shall be liable for, and shall indemnify (and keep indemnified) the Processor in respect of any and all action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and payments on a solicitor and client basis), or demand suffered or incurred by, awarded against, or agreed to be paid by, the Processor arising directly or in connection with:

a) any non-compliance by the Controller with the Data Protection Legislation;

b) any processing carried out by the Processor in accordance with instructions given by the Controller that infringe the Data Protection Legislation; or

c) any breach by the Controller of its obligations under this Agreement,

i) except to the extent that the Processor is liable under sub-Clause 8.2.

8.2 The Processor shall be liable for, and shall indemnify (and keep indemnified) the Controller in respect of any and all action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and payments on a solicitor and client basis), or demand suffered or incurred by, awarded against, or agreed to be paid by, the Controller arising directly or in connection with the Processor's processing activities that are subject to this Agreement:

a) only to the extent that the same results from the Processor's breach of, or non-compliance with, this Agreement, the Controller's instructions, or the Data Protection Legislation; and

b) not to the extent that the same is, or are contributed to, by any breach of this Agreement by the Controller.

8.3 The Controller shall not be entitled to claim back from the Processor any sums paid in compensation by the Controller in respect of any damage to the extent that the Controller is liable to indemnify the Processor under sub-Clause 8.1.

8.4 Nothing in this Agreement (and in particular, this Clause 8) shall relieve either Party of, or otherwise affect, the liability of either Party to any Data

Subject, or for any other breach of that Party’s direct obligations under the Data Protection Legislation. Furthermore, the Processor hereby acknowledges that it shall remain subject to the authority of the Commissioner and shall co-operate fully therewith, as required, and that failure to comply with its obligations as a Processor under the Data Protection Legislation may render it subject to the fines, penalties, and compensation requirements set out in the Data Protection Legislation.

9. Intellectual Property Rights

9.1 All copyright, database rights, and other intellectual property rights in the Personal Data (including but not limited to any updates, amendments, or adaptations to the Personal Data made by either the Controller or the Processor) shall belong to the Controller or to any other applicable third party from whom the Controller has obtained the Personal Data under licence (including, but not limited to, Data Subjects, where applicable). The Processor is licensed to use such Personal Data only for the purposes of providing the Services, and in accordance with this Agreement.

10. Confidentiality

10.1 The Processor shall maintain the Personal Data in confidence, and in particular, unless the Controller has given written consent for the Processor to do so, the Processor shall not disclose any Personal Data supplied to the Processor by, for, or on behalf of, the Controller to any third party. The Processor shall not process or make any use of any Personal Data supplied to it by the Controller otherwise than in connection with the provision of the Services to the Controller.

10.2 The Processor shall ensure that all personnel who are to access and/or process any of the Personal Data are contractually obliged to keep the Personal Data confidential.

10.3 The obligations set out in in this Clause 10 shall continue for a period of six years after the cessation of the provision of Services by the Processor to the Controller.

10.4 Nothing in this Agreement shall prevent either Party from complying with any requirement to disclose Personal Data where such disclosure is required by law. In such cases, the Party required to disclose shall notify the other Party of the disclosure requirements prior to disclosure, unless such notification is prohibited by law.

10.5 The controller agrees that their aggregated non-identifiable data is included and shared in the form of an online dashboard with all participating hospitals in each region able to view all the hospitals in their own region. The data cannot be downloaded from the dashboard

11. Subcontractors

11.1 The Processor shall not subcontract any of its obligations or rights under this Agreement without the prior written consent of the Controller.

11.2 If the Processor appoints a subcontractor (with the written consent of the Controller), the Processor shall:

a) enter into a written agreement with the subcontractor which shall impose upon the subcontractor the same obligations as are imposed upon the Processor by this Agreement and which shall permit both the Processor and the Controller to enforce those obligations;

b) ensure that the subcontractor complies fully with its obligations under that agreement and the Data Protection Legislation;

c) maintain control over all Personal Data transferred to the subcontractor; and

d) the agreement between the Processor and the subcontractor shall terminate automatically upon the termination or expiry of this Agreement for any reason.

11.3 In the event that a subcontractor fails to meet its obligations under any such agreement, the Processor shall remain fully liable to the Controller for failing to meet its obligations under this Agreement.

11.4 The Provider shall be deemed to have control legally over any Personal Data that is in the possession of or practically controlled by its subcontractors.

12. Deletion and/or Disposal of Personal Data

12.1 The Processor shall, at the written request of the Controller, delete or otherwise dispose of the Personal Data or return it to the Controller in the format(s) reasonably requested by the Controller within a reasonable time after the earlier of the following:

a) the end of the provision of the Services or

b) the processing of that Personal Data by the Processor is no longer required for the performance of the Processor's obligations under this Agreement.

12.2 Following the deletion, disposal, or return of the Personal Data under sub-Clause 12.1, the Processor shall delete or otherwise dispose of all further copies of the Personal Data that it holds, unless retention of such copies is required by law, in which case the Processor shall inform the Controller of such requirement(s) in writing.

12.3 All Personal Data to be deleted or disposed of under this Agreement shall be deleted or disposed of securely.

13. Consideration

13.1 The Processor accepts the obligations in this Agreement in consideration of the payment of £1 from the Controller, which the Processor hereby acknowledges.

14. Law and Jurisdiction

14.1 This Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall be governed by, and construed in accordance with, the laws of England and Wales.

14.2 Any dispute, controversy, proceedings or claim between the Parties relating to this Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall fall within the jurisdiction of the courts of England and Wales.

SIGNED for and on behalf of the Controller by:

Name, title of signee and organisation

____
Authorised Signature

Date: ____________

SIGNED for and on behalf of the Processor by:

Peter Carpenter, Service Delivery Director, Kent Surrey Sussex AHSN Limited

____
Authorised Signature

Date: ____________

SIGNED for and on behalf of the Processor by:

Ian Mylon, Chief Operating Officer, Unity Insights Limited

____
Authorised Signature

Date: ____________

15. Change History

Document version	Date	Amendments made	Status	Authorisation
1.0	01/05/2019	Initial GDPR compliant data processing agreement	Retired	NJ Birch
1.1	10/05/2019	Added / changed definitions in section 5, changed formatting in section 5.7, corrected a reference in section 13.1 and added cessation dates to Appendix A	Retired	NJ Birch
1.2	27/06/2019	Form fields added. Rewording of definitions.	Retired	NJ Birch
1.3	17/07/2019	Minor formatting changes	Retired	NJ Birch
1.4 - 1.7	18/07/2019	Removed extra blank column from sections 1 - 4 and other minor changes	Retired	NJ Birch
2.0	11/06/2021	Major revision taking into account the impact of Brexit and the UK GDPR etc.	Retired	NJ Birch
2.1	17/06/2021	Numbering of sub-sections adjusted in sections 9.e) and 13 and	Retired	NJ Birch
2.2	02/11/21	Review by KSS AHSN / Unity Insights contracting	Retired	F Craig
2.3	16/11/22	Added paragraph regarding sharing in region (10.5)	Working	J Rocliffe

SCHEDULE 1

Services

1. Receiving of Heart Failure audit data from the Controller.
2. Provision of Heart Failure audit analysis and dashboards using the data provided by the Controller, on a web-based platform (Tableau), commencing on the date of this Agreement.

SCHEDULE 2

Personal Data

Type of Personal Data	Category of Data Subject	Nature of Processing Carried Out	Purpose(s) of Processing	Duration of Processing
Local patient identifier (1.02) cm	Patient	Provision of Heart Failure and Heart Failure audit analysis and dashboards	To remove duplicates in the data (along with the date of discharge) to ensure that double counting does not occur; therefore maintaining data quality.	Monthly, for the duration of the Term of this agreement
Patient administration details, diagnosis, symptoms, long term conditions, treatment and follow up care	Patient	Provision of Heart Failure and Heart Failure audit analysis and dashboards	Analysis and reporting to the Controller	Monthly, for the duration of the Term of this agreement

SCHEDULE 3

Technical and Organisational Data Protection Measures

The following are the technical and organisational data protection measures referred to in Clause 4:

1. The Processor shall ensure that, in respect of all Personal Data it receives from or processes on behalf of the Controller, it maintains security measures to a standard appropriate to:

1.1 the harm that might result from unlawful or unauthorised processing or accidental loss, damage, or destruction of the Personal Data; and

1.2 the nature of the Personal Data.

2. In particular, the Processor shall:

2.1 have in place, and comply with, a security policy which:

a) defines security needs based on a risk assessment;

b) allocates responsibility for implementing the policy to a specific individual or personnel;

c) is provided to the Controller on or before the commencement of this Agreement;

d) is disseminated to all relevant staff; and

e) provides a mechanism for feedback and review.

2.2 ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice;

2.3 prevent unauthorised access to the Personal Data;

2.4 protect the Personal Data using pseudonymisation and encryption, where it is practical to do so;

2.5 ensure that its storage of Personal Data conforms with best industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled;

2.6 have secure methods in place for the transfer of Personal Data whether in physical form (for example, by using couriers rather than post) or electronic form;

2.7 password protect all computers and other devices on which Personal Data is stored, ensuring that all passwords are secure and that passwords are not shared under any circumstances;

2.8 take reasonable steps to ensure the reliability of personnel who have access to the Personal Data;

2.9 have in place methods for detecting and dealing with breaches of security (including loss, damage, or destruction of Personal Data) including:

a) the ability to identify which individuals have worked with specific Personal Data;

b) having a proper procedure in place for investigating and remedying breaches of the Data Protection Legislation; and

c) notifying the Controller as soon as any such security breach occurs.

2.10 have a secure procedure for backing up all electronic Personal Data and storing back-ups separately from originals;

2.11 have a secure method of disposal of unwanted Personal Data including for back-ups, disks, print-outs, and redundant equipment.