|  |
| --- |
|  |
| CONsultancy **AGREEMENT**  **(‘Agreement’)** |
| DATED INSERT (‘Agreement Date’) |
| *Between* |
| 1. INSERT   *and* |
| 1. Loughborough University |

CONTENTS

1 Interpretation and Defined Terms in this Agreement 3

2 Services 4

3 Substitute 4

4 Payment 5

5 Confidentiality 5

6 Publicity 5

7 Anti Corruption and Bribery Act 5

8 Intellectual Property 6

9 Term and Termination 7

10 Independent Consultant 7

11 Consultant’s obligations 8

12 Data Protection 9

13 Criminal Finances Act 9

14 Force Majeure 10

15 Third Party Rights 10

16 Entire Agreement 10

17 Assignment 10

18 Severability 10

19 Variation 10

20 Waiver 10

21 Notices 11

22 Disputes 11

23 Governing Law 11

Annex 1 13

Annex 2 14

Annex 3 15

CONsultancy **AGREEMENT**

Between:

1. INSERT NAME (Registered **Company No. INSERT) of** INSERT ADDRESS (the ‘Consultant’); and
2. Loughborough University of Epinal Way, Loughborough  
   Leicestershire, LE11 3TU (the ‘University’).

Each a ‘Party’ and together the ‘Parties’.

INTRODUCTION

1. The Consultant has certain skills and abilities in the field of INSERT that the University wishes to use.
2. The Consultant will provide the Services and the University will accept them on the terms of this Agreement.

Agreed Terms

# Interpretation and Defined Terms in this Agreement

In this Agreement, the terms set out below will have the following meanings:-

## **‘Arising IP’** means all (or any part) of the IP written, originated, conceived or made in the conduct of the Services by, or on behalf of, or jointly with the Consultant.

## **‘Background IP’** means any IP owned by either Party as at the Contract Start Date.

## **‘Business Day’** means any calendar day which is not a Saturday, Sunday or bank holiday in the United Kingdom.

## **‘Charges’** means any fees payable by the University to the Consultant under this Agreement as set out in **Annex 2** and all agreed expenses incurred by the Consultant in the provision of the Services for which the University is liable to repay the Consultant in accordance with **Annex 2.**

## **‘Contract Start Date’** means INSERT.

## **‘Contract Period’** means from the Contract Start Date until INSERT.

## **‘Confidential Information’** means information in whatever form (including without limitation, in written, oral, visual or electronic form or on any magnetic or optical disk or memory and wherever located) relating to the business, students, customers, clients, products, services, affairs and finances of the University for the time being confidential to the University and trade secrets including, without limitation, technical data and know-how relating to the business of the University or any of its suppliers, students, customers, clients, agents, consultants or business contacts, including (but not limited to) information that the Consultant creates, develops, receives or obtains in connection with the Engagement, whether or not such information is marked confidential.

## **’Data Protection Laws**’ shall be as defined in the Data Protection Annex.

## “**Data Protection Annex**” shall refer to Annex 3 to this Agreement.

## **‘Deliverables’** means the physical results of the Services.

## **‘Engagement'** means the engagement of the Consultant by the University on the terms of this Agreement.

## **‘Intellectual Property’** and **‘IP’** means all patents, registered designs, trademarks and service marks (whether registered or not), copyright, database rights, plant breeders rights, design right, know-how, information and all similar property including that subsisting (in any part of the world) in inventions, designs, performances, computer programs, semiconductor topographies, confidential information, business names, goodwill and the styles of presentation of goods or services and in applications for protection of them in any jurisdiction.

## **‘Services’** means the services to be provided to the University under this Agreement as described in **ANNEX 1**.

## **‘Substitute’** means a substitute employed by the Consultant under the terms of clause 3.

## **‘University Property'** means all documents, books, manuals, materials, records, correspondence, papers and information (on whatever media and wherever located) relating to the business or affairs of the University or its students, customers and business contacts, and any equipment, keys, hardware or software provided for the Consultant's use by the University during the Engagement and any data or documents (including copies) produced, maintained or stored by the Consultant on any computer system or other electronic equipment during the term of this Agreement.

## The headings in this Agreement are for ease of reference only and shall not affect its interpretation.

## References to ‘including’ in this Agreement in the context of a list or description of items shall be construed as meaning ‘including without limiting the generality of the foregoing’, such that the items following are merely examples of items which are included and/or items which are identified as being included for the avoidance of any doubt as to their inclusion, and such items are not descriptive of the class of items which may be included.

# Services

## The Consultant will provide the Services with effect from the Contract Start Date for a period of [ ] years or until terminated under Clause 9.

## Nothing in this agreement shall prevent the Consultant from being engaged, concerned or having any financial interest in any capacity in any other business trade profession or occupation during the Engagement provided that the activity does not cause a breach of any of the Consultant’s obligations under this Agreement.

# Substitute

## The Consultant may, with the prior written approval of the University and subject to the following proviso, appoint a suitably qualified and skilled Substitute to perform the Services on his behalf, provided that the Substitute shall be required to enter into direct undertakings with the University, including with regard to confidentiality. If the University accepts the Substitute, the Consultant shall continue to invoice the University in accordance with clause 4 and shall be responsible for the remuneration of the Substitute. For the avoidance of doubt, the Consultant will continue to be subject to all duties and obligations under this Agreement for the duration of the appointment of the Substitute.

# Payment

## Invoices shall be sent to address detailed on the subsequent purchase orders.

## The Consultant may submit an invoice at any time after the Contract Period, unless otherwise stated in Annex 2.

## Where the Consultant submits an invoice to the University in accordance with clauses 4.1 and 4.2, the University will consider and verify that invoice in a timely fashion.

## The University shall pay the Consultant any sums due under such an invoice no later than a period of 30 days from the date on which the University has determined that the invoice is valid and undisputed. The University will also pay VAT at the prevailing rate, if applicable.

## Where the University fails to comply with clause 4.3 and there is an undue delay in considering and verifying the invoice, the invoice shall be regarded as valid and undisputed for the purposes of clause 4.4 after a reasonable time has passed.

# Confidentiality

## The Consultant will not either during the Engagement or at any time thereafter use or disclose to any third party (and shall use his best endeavours to prevent any such publication or disclosure) any Confidential Information.

## The obligations in Clause 5.1 shall not apply or shall cease to apply to Confidential Information which:

### is in or comes into the public domain other than by reason of a breach of this Agreement; or

### is required to be disclosed by law or a court or other competent authority.

## Upon termination of this Agreement for whatever reason, or at any time during the Engagement at the written request of the University, the Consultant will deliver up to the University all University Property.

# Publicity

## The Consultant will not use the name of the University, nor of any member of the University's staff, in any publicity, advertising or news release without the prior written approval of an authorised representative of the University. Other than for annual reporting purposes, the University will not use the name of the Consultant, nor any employee of the Consultant, in any publicity without the prior written approval of the Consultant.

# Anti Corruption and Bribery Act

## Each Party:

### shall comply with all applicable laws, statutes and regulations relating to anti-bribery and anti-corruption including, the Bribery Act 2010 and not  engage in any activity, practice or conduct or knowingly allow anyone connected to it to do so which would constitute an offence under the Bribery Act 2010;

### warrants and represents (without limiting the generality of 7.1.1) to the other that it has not offered to give or agreed to give to any person any gift or consideration of any kind as an inducement or reward for doing or forbearing to do or for having done or forborne to do any act in relation to the obtaining or execution of this Agreement or for showing or forbearing to show favour or disfavour to any person in relation to this Agreement;

### shall ensure that any person who is performing services or providing goods in connection with this Agreement abides by the terms of this Agreement.

## Breach of this Clause shall be deemed a material breach of this Agreement allowing the non-defaulting party to terminate this Agreement immediately on notice.

# Intellectual Property

## All Background IP used in connection with the Services shall remain the property of the Party introducing it.

## All Arising IP will vest in the University. All such Arising IP (both existing and future) is hereby assigned by the Consultant to the University with full title guarantee. This shall include any and all Arising IP developed by a Substitute.

## The Consultant will promptly disclose to the University any and all Background IP it uses in the provision of the Services and any and all Arising IP created as a result of this Agreement.

## The University shall have the option to take a licence of the Consultant’s Background IP to the extent required to enable the University to exploit the Arising IP. If the University wishes to exercise its option to take a licence of the Consultant's Background IP, it must serve written notice on the Consultant stating the scope of the Background IP of which it wishes to obtain a licence.

## Upon the notice under clause 8.4 being served, the Consultant shall immediately licence the Background IP specified in that notice to the University by way of an irrevocable, royalty free, worldwide licence with the right to grant sublicenses to use the Background IP in conjunction with the Arising IP.

## The Party applying for patent or other IP protection for any Arising IP will pay all costs associated with the application. The Parties will cooperate with each other in executing such documents as may be reasonably required in the prosecution of such application(s) and to ensure that such application(s) will cover, to each Party’s reasonable knowledge, all items of commercial interest and importance.

## The Consultant hereby assigns with full title guarantee to the University all right, title and interest it has (both existing and future) in any and all Deliverables which it supplies to the University and which it is intended will be retained by the University.

## The Consultant irrevocably and unconditionally waives and shall procure the irrevocable and unconditional waiver in favour of the University of any and all moral rights conferred by Part I of the Copyright Designs and Patents Act 1988 or any similar rights anywhere in the world in relation to any Deliverable.

## The Consultant shall at the request of the University and at the entire cost of the University:

### execute any further documents and/or deeds and do any such things as the University may require to enable the University to secure the delivery of information and the benefit of the rights assigned or held in trust in accordance with this clause 8; and/or

### take such action as the University may reasonably require to assist the University in bringing or defending any proceedings relating to the Background IP licensed to it pursuant to this Agreement and any Arising IP.

# Term and Termination

## This Agreement will continue until the end of the Contract Period unless terminated in accordance with this Clause 9 or by the University giving written notice under Clause 9.2 or by mutual written agreement of the Parties under Clause 9.3.

## The University may terminate this Agreement if written notice to the Consultant is given, specifying the date from which termination shall be effective. In such event the University shall make reasonable payment to the Consultant for all work performed prior to the date of termination and any approved additional costs necessarily incurred by the Consultant as a direct result of such termination.

## Either Party may terminate this Agreement forthwith if the other Party commits a material breach of this Agreement which has not been remedied after 28 days written notice of the breach (such notice expressly referring to possible termination of this Agreement).

## The University may terminate this Agreement forthwith if the Consultant is declared bankrupt or makes any arrangement with or for the benefit of his creditors or has a county court administration order made against him under the County Court Act 1984.

## Subject to Clause 9.6 below, termination of the Agreement by either Party for any reason shall not affect the rights and obligations of the Parties accrued prior to the effective date of termination of this Agreement. Those clauses of this Agreement which are expressly or impliedly intended to continue after termination shall continue in effect after termination.

## The obligations of the Parties under this Agreement impose no further obligation on either Party:

### to prescribe, provide favourable status for, or otherwise support the other Party’s or a third party’s products or services; or

### to supply services or to provide anything other than that which is set out in this Agreement.

# Independent Consultant

## Neither Party is authorised or empowered to act as agent for the other for any purpose and shall not on behalf of the other enter into any contract, warranty, or representation as to any matter. Neither shall be bound by the acts or conduct of the other.

## The relationship of the Consultant to the University will be that of an Independent contractor and nothing in this Agreement shall render him an employee worker agent or partner of the University and the Consultant shall not hold himself out as such.

## This Agreement constitutes a contract for the provision of services and is not a contract of employment and accordingly the Consultant shall be fully responsible for and shall indemnify the University for and in respect of:

### Any income tax, national insurance or social security contributions and any other liability deduction contribution assessment or claim arising from or made in connection with the performance of the Services. The Consultant shall further indemnify the University against all reasonable costs expenses and any penalty fine or interest incurred or payable by the Consultant in connection with or in consequence of any such liability deduction contribution assessment or claim, other than where the latter arise out of the University's negligence or wilful default.

### Any liability arising from any employment related claim or any claim based on worker status (including reasonable costs and expenses) brought by the Consultant or any Substitute against the University arising out of or in connection with the provision of the Services.

## The University may at its discretion satisfy such indemnity (in whole or in part) by way of deduction from any payments due to the Consultant.

# Consultant’s obligations

## The Consultant shall:

### deliver the Services with the care, skill and diligence required in accordance with best practice in the Consultant’s industry, profession or trade, using all reasonable endeavours to ensure the accuracy of the work performed and any information and results given;

### comply with all applicable laws, statutes and regulations;

### use best endeavours to promote the interests of the University;

### properly give to the University all such information and reports as it may reasonably require in connection with the provision of the Services;

### notify the University as soon as is reasonably practicable if the Consultant is unable to provide the Services due to illness or injury. For the avoidance of doubt, the charges shall not be payable in respect of any period during which the Services are not provided;

### comply with all reasonable standards of health and safety and comply with the University’s health and safety procedures from time to time in force at the premises where the Services are provided and report to the University any unsafe working conditions or practices;

### comply with the University’s policies on [social media/use of information and communication systems/anti-harassment and bullying/etc].

## The Consultant shall have personal liability for and shall indemnify the University for any loss/ liability /cost (including reasonable legal costs) damages or expenses arising from any breach by the Consultant or any Substitute of the terms of this Agreement including any negligent or reckless act, omission or default in the provision of the Services and undertakes that he will:

### take out and maintain professional indemnity/public liability insurance with a reputable insurance company, providing a minimum cover of £10,000,000; (Procurement ability to vary as appropriate)

### maintain Professional Indemnity insurance cover for the Services for the duration of this Agreement and for a period of six (6) years after completion of the Services;

### supply the University with copies of current certificates of insurance for the duration of the Agreement;

### notify the insurers of the University’s interest and cause the interest to be noticed on the relevant insurance policies; and

### comply with all terms and conditions of the relevant insurance policies at all times and notify the University without delay if he becomes aware of any reason why the cover under the relevant insurance policies may lapse or not be renewed or be changed in any material manner.

# Data Protection

## The Consultant consents to:

### The University holding and processing personal data (as defined in the Data Protection Laws) relating to him for legal, personnel, administrative and management purposes;

### the University making such personal data available to regulatory authorities as required under the Data Protection Laws; and

### the transfer of such information to the University’s business contacts outside the European Economic Area in order to further the commercial interests of the University, provided always that the transfer is permitted under the Data Protection Laws.

## The Consultant shall comply with the Data Protection Annex when processing University Data (as defined in the Data Protection Annex).

# Criminal Finances Act

## The Consultant shall have in place processes, procedures, checks and balances in order to ensure it is able to comply with the requirements of the CFA. The Consultant shall:

### Not engage in any activity, practice or conduct which would constitute either:

#### A UK tax evasion facilitation offence under section 45(1) of the Criminal Finances Act 2017; or

#### a foreign tax evasion facilitation offence under section 46(1) of the Criminal Finances Act 2017;

### maintain in place throughout the term of this agreement such procedures as are reasonable to prevent the facilitation of tax evasion by a Substitute; and

### promptly report to the University any request or demand from a third party to facilitate the evasion of tax within the meaning of Part 3 of the Criminal Finances Act 2017, in connection with the performance of this agreement.

## The Consultant shall cooperate with the University in full with regards to any audits it may reasonably undertake in order to examine the processes and practices of the Consultant in the context of the requirements of the Criminal Finances Act 2017.

## Breach of this Clause 13 shall be deemed a material breach of this Agreement allowing the University to terminate this Agreement immediately on notice.

# Force Majeure

## For the purposes of this Agreement, Force Majeure Event means an event beyond the reasonable control of the party which is affected by it including but not limited to strikes, lock-outs or other industrial disputes, failure of a utility service or transport network, act of God, war, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, storm or default of suppliers or sub-contractors.

## Any failure or delay by either Party in the performance of its obligations pursuant to this Agreement which is due to a Force Majeure Event will not be deemed a default of this Agreement or a ground for termination. If a force majeure event affecting the Consultant continues for more than 30 days, the University shall have the right to terminate this Agreement immediately upon written notice to the Consultant.

# Third Party Rights

## The Parties to this Agreement do not intend that any of its terms will be enforceable by virtue of the Contracts (Rights of Third Parties) Act 1999 by any person not a Party to it.

# Entire Agreement

## Each Party acknowledges that this Agreement contains the whole agreement between the Parties in respect of its subject matter and supersedes all prior arrangements, agreements, promises, statements, representations, assurances, warranties and understandings between them relating to the subject matter.

# Assignment

## This Agreement shall not be assigned by either Party without the prior written consent of the other.

# Severability

## If any provision of this Agreement is declared void or unenforceable, such provision shall be severed from this Agreement, which shall otherwise remain in full force and effect.

# Variation

## Any variation to this Agreement (and/or the Services) shall be in writing and signed by the parties (or their authorised signatories).

# Waiver

## No failure, delay, relaxation or indulgence on the part of either Party in exercising or partial exercise of any right hereunder shall operate as a waiver of such rights.

# Notices

## Any notice, demand or communication in connection with this Agreement will be in writing and may be delivered by hand, Special Delivery post or by email addressed to the recipient at the address below (or another person which the recipient has notified in writing to the sender in accordance with this Clause 20.1, to be received by the sender not less than seven days before the notice is despatched).

### For the University – to INSERT NAME AND CONTACT DETAILS OF THE SENIOR RESPONSIBLE OWNER OF THE CONTRACT WITHIN THE DEPARTMENT

### For the Consultant – to INSERT

## The notice, demand or communication will be deemed to have been duly served:

### if delivered by hand, at the time of delivery;

### if delivered by Special Delivery post, 48 hours after being posted (excluding days other than business days in England).

### [If delivered by email, at the time of transmission unless sent outside normal business working hours, in which case, on the next following business day, provided that a confirmatory copy is sent by Special Delivery post or by hand by the end of the next business day.]

## The contacts for academic issues and day to day management of the Services will be:-

### For the University: - INSERT.

### For the Consultant: - INSERT

# Disputes

## All disputes will initially be referred by either Party to a representative of each Party responsible for the overall performance of this Agreement, who will meet as soon as reasonably practicable to discuss the dispute.

## Any dispute arising out of this Agreement which the Parties are unable to resolve within five Business days, shall be determined by the appointment of a single arbitrator to be agreed between the parties, or failing agreement within fourteen days, after either party has given to the other a written request to concur in the appointment of an arbitrator, by an arbitrator to be appointed by the President or Deputy President of the Chartered Institute of Arbitrators.

# Governing Law

## This Agreement and any dispute or claim arising out of it is governed by the law of England and Wales and subject to Clause 21.1 the Parties submit to the exclusive jurisdiction of the courts of England and Wales.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Signed** |  |  | **Signed** |  |
| *for the Consultant* | |  | *Authorised Signature for and on behalf of Loughborough University* | |
| **Name:** |  |  | **Name:** |  |
|  |  |  |  |  |
| **Position:** |  |  | **Position:** |  |
|  |  |  |  |  |
| **Dated:** |  |  | **Dated:** |  |

Annex 1

**The Services**

[The following Services will be provided]

Annex 2

**Charges**

Fee: **Total: GBP £INSERT**

[The Fee paid will be subject to the maximum funding available of [ ], at a daily rate of [£]

All costs exclude applicable VAT.

# Annex 3

DATA PROTECTION SCHEDULE

**WHERE THE CONSULTANT PROCESSES PERSONAL DATA, THE TERMS SET OUT BELOW SHALL APPLY:**

1. **DEFINITIONS**

In this Schedule, capitalised terms which are not defined below shall have the meanings attributed to them in the Conditions. The following words shall have the following meanings:

|  |  |
| --- | --- |
| **“Contract”** | means the main Contract to be entered into between the University and the Consultant which expressly incorporates this Data Protection Schedule. |
| **“Data Controller”** | is as defined in applicable Data Protection Laws; |
| **“Data Processor/s”** | is as defined in applicable Data Protection Laws; |
| **“Data Protection Authority”** | means the Information Commissioner’s Office, or any other relevant local governmental or other official regulator(s) responsible for enforcement of the Data Protection Laws from time to time in relation to the University; |
| **“Data Protection Laws ”** | means all applicable laws and regulations relating to the processing of Personal Data and privacy including the Data Protection Act 2018, the General Data Protection Regulation 2016 (EU) 2016/679, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) and the Electronic Communications Data Protection Directive (2002/58/EC), including any relevant replacement/subsequent European and/or UK legislation as may come into force from time to time and any successor legislation to the same, or, in the event that the UK leaves the European Union, all legislation enacted in the UK in respect of the protection of personal data, together with all codes of practice and other guidance on the foregoing issued by any relevant Data Protection Authority or regulatory body, all as amended from time to time; |
| **“Data Subject”** | means any individual who is the subject of any Personal Data; |
| **“Data Transfer Contract”** | meansthe standard contractual clauses for Data Processors established in third countries pursuant to the Commission Decision (2010/87/EU) of 5 February 2010 under the EU Directive (95/46/EC) or any other relevant/subsequent Commission decision as may replace Commission Decision (2010/87/EU) from time to time together with such other clauses as the University shall in its sole discretion deem appropriate and as required under applicable Data Protection Laws; |
| **“Personal Data”** | is as defined in applicable Data Protection Laws; |
| **“Personnel”** | means any person employed or engaged by or on behalf of the Consultant who is engaged in the provision of the Services to University and/or assists the Consultant with its performance of its obligations under the Contract, including Personnel employed or engaged by a Third-Party; |
| **“Process” and other derivations such as “Processed” and “Processing”** | means any use of or processing applied to any Personal Data and includes “process” or “processing” as defined in applicable Data Protection Laws. For the avoidance of doubt, this includes, without limitation, collecting, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying Personal Data; |
| **“Schedule”** | means this Data Protection Schedule; |
| **“Third Party/Parties”** | any agent, subcontractor or Substitute for the Consultant engaged by the Consultant in relation to the provision of the Services to the University and/or who assists Consultant with its performance of its obligations under the Contract in whole or part and who Processes Personal Data in doing so. |
| **“University Data”** | means all Personal Data belonging to the University which is from time to time Processed (as defined below) under this Contract by the Consultant and/or on the Consultant’s behalf including but not limited to all electronic data or information submitted by the University and/or the users of the University’s information technology systems and any Personal Data provided by or on behalf of the University and any Personal Data in respect of any student of the University. A schedule of University Data at appendix 2 will identify all the categories of University Data captured. |

1. CONSULTANT AS DATA PROCESSOR
   1. In respect of the provision of the Services the Parties agree and acknowledge for the purposes of the Data Protection Laws, the University is the Data Controller and the Consultant is a Data Processor in respect of the University Data.
2. CONSULTANT’S OBLIGATIONS TO ACT ON INSTRUCTIONS
   1. Act on Instructions

The Consultant hereby warrants and undertakes on a continuing basis that it shall and that it shall procure that any Third Party shall:

* + 1. only Process the University Data in order to provide the Services and then strictly only in accordance with the terms of the Contract, this Schedule and such other written instructions received from the University from time to time relating to the University Data and shall not process the University Data for any other purpose;
    2. promptly comply with any request from the University requiring **the Consultant** to amend, transfer or delete any University Data;
    3. promptly and fully cooperate with and assist the University in relation to any reasonable request for cooperation and/or assistance and/or information relating to its Processing of the University Data;
    4. at the University’s request, promptly provide it with a copy of all University Data held by the Consultant in the format and on the media reasonably specified by the University;
    5. keep full and proper records in accordance with the accountability requirements of the Data Protection Laws;
    6. ensure that the University Data shall only be accessible by the Consultant’s Personnel and/or Third Parties to the extent they need to know or require access to it for the purposes of properly performing their duties in relation to the Contract and who, where relevant, understand the confidentiality of such University Data and who are contractually bound to maintain its confidentiality.
    7. Ensure that all Personnel are aware of the Consultant’s duties and their direct duties and obligations under the Data Protection Laws, this Schedule and the Contract.
    8. not cause the University to be in breach of any part of the Data Protection Laws whether by reason of an act or omission by it or them, or by any of its or their directors, officers, staff, employees or Third Parties;
    9. not allow any Third Party to access the University Data except to the extent that the Consultant obtains the prior written consent of the University and **PROVIDED ALWAYS** that the following conditions shall apply to such consent and after such consent is given:
       1. such Third Parties shall not be entitled to subcontract further in whole or in part or to allow any additional third party access to the University Data;
       2. the Third Party’s appointment is otherwise on the same basis and terms as in this **paragraph 3** and the Consultant shall enter into a written contract with the Third Party accordingly and on terms at least as restrictive as those set out in this Schedule, prior to them processing any University Data and the contract shall be provided to the University and shall be subject to the University’s express prior approval;
       3. the Consultant shall procure compliance by the Third Party with these terms and shall be responsible for the acts and omissions of such Third Party and shall fully indemnify the University against all losses, damages, charges, fines, costs, or expenses and other liabilities (including without limitation legal fees) incurred by, awarded against or agreed to be paid by the University arising from any act or omission of any Third Party; and
       4. the Consultant shall comply with such other conditions as the University may impose in relation to its consent from time to time.
    10. the Consultant shall follow its archiving procedures for University Data as set out in the University’s Back-Up Policy (available on request from the University), as such document may be amended by the University in its sole discretion from time to time.
    11. If at any time the Consultant suspects or has reason to believe that any University Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Consultant shall notify the University immediately and inform the University of the remedial action it proposes to take.
    12. In addition to any other rights or remedies the University may have, in the event of any loss or damage to the University Data, the Consultant shall procure the restoration of the lost or damaged University Data from the latest back-up of such University Data maintained by it] in accordance with the University’s Back-Up Policy (available on request from the University), or compensate the University for so doing;
    13. the Consultant shall, in providing the Service(s), comply with the University’s Privacy and Security Policy (available on request from the University) as amended from time to time by the University in its sole discretion.
    14. the Consultant shall at all times in respect of Personal Data of which the University is the Data Controller comply with obligations equivalent to those set out in the Data Protection Laws.
  1. **Security Measures**

The Consultant warrants and undertakes on a continuing basis that it shall, and that it shall procure that any Third Parties it contracts with shall:

* + 1. put in place and securely maintain appropriate technical infrastructure and organisational measures in compliance with the Data Protection Laws and recognised best practice, sufficient to protect against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access to the University Data (including, without limitation the measures set out in **Appendix 1**); and
    2. take reasonable steps to ensure the continuing reliability and capability of Personnel who have access to University Data and to ensure they are regularly trained and tested in information security sufficient to maintain awareness of their obligations in relation to Personal Data under this Schedule, the Contract and the Data Protection Laws.
  1. **Data Breach**

The Consultant warrants and undertakes on a continuing basis that it shall and that it shall procure that any Third Party shall:

* + 1. notify the University within 24 hours of the occurrence of any actual or suspected, threatened or ‘near miss’ incident of accidental, or unlawful, destruction, or accidental loss, alteration, unauthorised or accidental disclosure of or access to the University Data or any other breach of security in relation to the University Data or breach of any provision of the Data Protection Laws leading to the same (a “**Data Breach”**).
    2. thereafter provide the University within 2 Business Days with all relevant information in its or their possession as required by the University to comply with any informal or formal management and reporting obligations recommended or required by Data Protection Laws concerning any such Data Breach, including: type of Personal Data or other information involved; number of records involved/Data Subjects affected; circumstances of Data Breach; mitigation and actions taken; investigation details; details of reports to and reactions from other relevant bodies of the breach; and remedial action taken and intended to be taken to avoid repeats);
    3. not make any announcement or publish or otherwise authorise any broadcast of any notice or information about a Data Breach, including to a Data Protection Authority, (a **“Breach Notice”**) without the prior written consent of and prior written approval by the University of the content, media and timing of the Breach Notice (if any).
  1. **Treatment of Personal Data**

The Consultant warrants and undertakes on a continuing basis that it shall and that it shall procure that all Third Parties shall fully comply at all times with the Data Protection Laws in respect of its and/or the Third Parties’ Processing of the University Data and in particular shall ensure all University Data inputted or recorded is accurate and up to date (to the extent within the Consultant’s or Third Party’s control) and that such University Data is only retained in accordance with the University’s data retention policy (available on request from the University).

* 1. **Audit**

Subject to the University and its auditors or other appointed professionals entering into reasonable confidentiality obligations, the Consultant warrants and undertakes on a continuing basis that it shall and that it shall procure that all Third Parties shall at any time upon request of the University, on reasonable notice and during regular business hours and at no cost to the University:

* + 1. ensure that its and/or their staff, employees, directors, agents and other Personnel are made available to the University and its auditors or other professionals (whether internal and/or external);
    2. provide all such persons with access to all relevant information (whether in electronic or hard copy form) relating to its Processing of the University Data and/or the performance of its obligations under this Schedule together with all premises where the University Data is Processed;
    3. procure that Personnel and all persons employed or engaged by any Third Party provide all reasonable co-operation and assistance to the University;
    4. ensure any vulnerabilities identified by any audits or penetration tests carried out by the Personnel, Third Parties, or those employed or engaged by Third Parties, on their own respective IT infrastructure, are notified to the University if they have not been remediated within one month of the original identification of the vulnerability;

as may be necessary in the reasonable opinion of the University to permit an accurate and complete assessment of the Consultant’s compliance with its obligations under this Schedule.

1. **REQUESTS FROM DATA SUBJECTS AND REGULATOR(S)**
   1. The Consultant warrants and undertakes that it shall, and shall procure that all Third Parties shall, notify the University within 2 Business Days, at no cost to the University, of any complaint by a Data Subject in respect of his Personal Data or any request received from a Data Subject to exercise his Data Subject rights under the Data Protection Legislation, or of any other communication relating directly or indirectly to the Processing of any University Data in connection with this Contract and provide all details of such complaint, request or communication to the University and promptly and fully cooperate and assist the University in relation to any such request or communication.
   2. Neither the Consultant nor any Third Party shall respond directly to any request by a Data Subject for access to their Personal Data, to any complaint by a Data Subject in relation to the Processing of their Personal Data, or (unless and to the extent required by law) any communication by a Data Protection Authority to them in relation to any University Data, in each case unless expressly approved in writing in advance by the University.
2. DATA TRANSFERS
   1. Subject to the terms of this Contract the Consultant warrants and undertakes on a continuing basis that it shall not, and that it shall procure that the Third Parties shall not, cause or permit the University Data to be Processed or transferred outside the European Economic Area (the **“EEA”**) without the prior written consent of the University and shall comply with the conditions imposed on such consent by the University as set out in **paragraph 5.2**.
   2. The Consultant warrants and undertakes on a continuing basis that should it obtain the prior written consent referred to in **paragraph 5.1** prior to any Processing of University Data outside the EEA and/or to any transfer of University Data outside the EEA:
      1. Where the Consultant wishes to use a Third Party outside the EEA or who will Process the University Data outside of the EEA, the Consultant shall ensure that either:
         1. The Third Party is located in a jurisdiction which affords an adequate level of protection to Data Subjects as regards the protection of their Personal Data, in accordance with the Data Protection laws; or
         2. prior to any transfer or processing each relevant Third Party enters into a Data Transfer Agreement with the University and the Consultant, at no additional cost to the University and to include such terms as the University shall, in its sole discretion, deem reasonable, appropriate or necessary;
      2. it shall provide a copy of each such executed Data Transfer Agreement to the University in advance of any such transfer.
      3. the Consultant shall procure the compliance of such Third Parties with the terms of the relevant Data Transfer Agreement.
      4. The Consultant shall at all times remain responsible for the acts and omissions of the Third Parties it contracts with in relation to the University Data.
3. CONSEQUENCES OF EXPIRY AND TERMINATION
   1. The Consultant will liaise with the University in the 3 month period prior to any termination or expiry of the Contract to ascertain the University’s preference and requirements (including details, format, media, method, timing and security) in relation to the secure return to it (or as it directs) of all or part of the University Data (or, the secure deletion or destruction of all or part of the University Data). If it is not possible for this to be carried out prior to termination or expiry, the Consultant shall cooperate with the University about such preference and requirements as soon as possible on termination or expiry.
   2. The Consultant shall fully cooperate and comply with the preferences and requirements of the University pursuant to **paragraph 6.1**. The Consultant shall also procure that Third Parties fully comply with these preferences and requirements.
   3. Subject to **paragraph 6.4**, the parties agree that:
      1. any deletion or destruction of University Data pursuant to **paragraph 6.1** shall be permanent and shall secure deletion of all requested University Data, being all electronic copies of it (in whole or in part) on its IT systems, equipment and any mobile devices, and complete and secure destruction of all hard copies of it (in whole or in part);
      2. any return of University Data pursuant to **paragraph 6.1** shall be the secure return (as required by the University) of all requested University Data in both electronic and hard copy formats (in whole or in part); and
      3. The Consultant shall certify in writing to the University that it has complied with **paragraphs 6.1, 6.2, 6.3.1 and 6.3.2** by itself and all Third Parties within 1 month of being requested to do so by the University following termination or expiry of the Contract.
   4. If the Consultant is required by law to retain University Data post termination or expiry and cannot return or destroy it in accordance with **paragraph 6.1**, it shall
      1. immediately notify the University in writing of the relevant University Data and the reason it must be retained and the required period of retention;
      2. be entitled to retain a single copy of such University Data;
      3. observe all the requirements of Data Protection Laws in relation to such University Data that is retained;
      4. only Process such University Data in accordance with the specific purposes and for the specific period for which the Consultant is under a legal duty to retain it;
      5. at the end of such period, securely and promptly destroy the University Data within 7 days and certify to the University in writing that it has done so; and
      6. promptly upon request provide to the University such information as is reasonably necessary to enable the University to satisfy itself of compliance by the Consultant and all Third Parties with this **paragraph 6**.

This **paragraph** shall continue in effect following termination or expiry of this Contract.

1. **INDEMNITY**
   1. The Consultant shall, at all times during and after the termination or expiry of this Contract, indemnify the University, keep the University indemnified and hold the University harmless from and against all losses, damages, charges, fines, costs, or expenses and other liabilities (including without limitation legal fees) incurred by, awarded against or agreed to be paid by the University arising from any breach of the Consultant’s obligations under this Schedule.
   2. Notwithstanding any other provision of this Schedule or the Contract, Consultant’s liability under the indemnity at **paragraph 7.1** shall not be subject to any exclusions or limitations of liability.
   3. The Consultant shall take out insurance sufficient to cover any payment that may be required under this paragraph 7 and produce the policy and receipt for premium paid, to the University on request.
2. **TRAINING**
   1. The Consultant will ensure that all Personnel are appropriately trained to Process Personal Data at all times;
   2. The Consultant will ensure that only those staff trained in Processing Personal Data will Process Personal Data in the provision of the Services.

Appendix 1

Security Measures

### ORGANISATION OF INFORMATION SECURITY

### Internal organisation

The Consultant will organise and allocate internal roles and responsibilities covering information security sufficient to ensure that any exposure to risk is minimised and to ensure compliance with the Data Protection Laws.

* 1. **Mobile devices and teleworking**

The Consultant will ensure security policies and controls are in place for mobile devices (such as laptops, tablet PCs, wearable ICT devices, smartphones, USB gadgets and other connected items) and teleworking (such as telecommuting, working-from home, telecommuting, and remote/virtual workplaces).

1. **HUMAN RESOURCE SECURITY**

**2.1  Prior to employment**

The Consultant will ensure security responsibilities are taken into account when recruiting permanent employees, Consultants and temporary staff (*e.g*. through adequate job descriptions, pre-employment screening) and included in contracts (*e.g*. terms and conditions of employment and other signed Contracts on security roles and responsibilities) whether or not it is intended such persons shall be Personnel.

#### **2.2 During employment**

The Consultant will ensure that all Personnel, employees and Consultants are appropriately trained in relation to their and the Consultant’s obligations under the Data Protection Laws and are made aware of and motivated to comply with their information security obligations under this Contract.  A formal disciplinary process should be in place to handle any Data Breach or other security breach. In the event that a Data Breach or other security breach occurs the University should be notified of that Data Breach and/or security breach (as appropriate), the circumstances, surrounding the Data Breach and/or security breach (as appropriate), any employee’s involvement or suspected involvement in any such Data Breach and/or security breach (as appropriate) and the disciplinary process.

#### **2.3  Termination and change of employment**

The Consultant will ensure data security aspects of an employee’s exit or significant changes of roles are managed. The Consultant will ensure exiting employees and Personnel:

1. Return all corporate information
2. Return all corporate equipment,
3. Update access rights,

are aware of their ongoing obligations under the Data Protection Laws, privacy laws and their contractual terms.

1. **ASSET MANAGEMENT**
   1. **Responsibility for assets**
      1. The Consultant will ensure that all information assets including but not limited to the University Data are inventoried and those with custody, control or responsibility for those assets, are identified and held clearly accountable for their security.
      2. The Consultant will ensure that it has in place appropriate ‘Acceptable use’ policies, that these are clearly defined, and that all assets, including but not limited to the University Data and all devices on which the University Data has been stored or Processed are returned when Personnel leave employment or engagement of the Consultant or any Third Party.
   2. **Information Classification**

The Consultant will ensure that all University Data is classified and labelled by those with custody, control or responsibility for it according to the appropriate security protection for such University Data, and that it is at all times handled appropriately and in accordance with its obligations under the Schedule, the Contract and the Data Protection Laws.

* 1. **Media handling**

### The Consultant will ensure that all information storage media is recorded, managed, controlled, moved and disposed of in such a way that the University Data is not compromised.

### **ACCESS CONTROL**

### **Business requirements of access control**

The Consultant’s requirements to control access to information assets and University Data should be clearly documented in an access control policy and appropriate procedures put in place. Furthermore, network access and connections will need to be restricted to ensure security of the University Data.

* 1. **Internal user access management**

The allocation of internal access rights to Personnel and in relation to other services not connected with the Service(s), other users shall be strictly controlled from initial user registration through to removal of access rights when no longer required, including special restrictions for privileged access rights and the management of passwords, or other authentication information, plus regular reviews and updates of access rights.

### **4.3  User responsibilities**

Personnel and where appropriate other internal users, will need to be made aware of their responsibilities towards maintaining effective access controls *e.g*. choosing strong passwords and keeping them confidential.

### **4.4 System and application access control**

Information access should be restricted in accordance with the access control policy referred to in paragraph 4.1 above e.g. through secure log-on, password/authentication management, control over privileged utilities and restricted access to program source code.

1. **CRYPTOGRAPHY**

### **5.1  Cryptographic controls**

The Consultant should put in place an appropriate policy on the use of encryption, plus cryptographic authentication and integrity controls such as digital signatures and message authentication codes, and cryptographic key management.

1. **PHYSICAL AND ENVIRONMENTAL SECURITY**

**6.1  Secure areas**

The Consultant must ensure that there are defined physical perimeters and barriers, with physical entry controls and working procedures, to protect the premises, offices, rooms, delivery/loading areas *etc* of all areas in which the University Data are stored or Processed*,* against unauthorised access.  The Consultant should seek specialist advice in order to put in place appropriate measures to mitigate the risk of and protect against fires, floods, earthquakes, bombs *etc.*

#### **6.2  Equipment security**

For the purposes of the annex “Equipment” shall mean the ICT equipment, storage media and any other physical equipment used for the Processing or storage of University Data plus supporting utilities, (such as power and air conditioning) and cabling. All Equipment should be secured and maintained. Equipment and University Data should not be taken off-site unless expressly authorised by the Consultant and must be adequately protected both on and off-site.  Any University Data contained on any Equipment must be securely destroyed prior to such Equipment being disposed of or re-used.  Unattended Equipment must be secured.

1. **OPERATIONS MANAGEMENT**

### **7.1  Operational procedures and responsibilities**

The Consultant shall ensure that all IT operating responsibilities and procedures are fully documented. Changes to IT facilities, systems or any Equipment should be controlled by structured and documented change management process. The Consultant should at all times manage the capacity and performance of all IT facilities, systems and the Equipment used in relation to the provision of the services or the Processing of any University Data shall be kept separate from any development, test and operational systems.

### **7.2  Protection from malware**

Malware controls are required on all IT facilities and Equipment including both servers and end-user devices in order to provide protection from malware, which, for the avoidance of any doubt includes ensuring user awareness.

### **7.3  Backup**

### The Consultant shall put in place and operate a back-up policy for the protection of the University Data and to ensure compliance with the Schedule. Such backup policy should include, but not be limited to a requirement that appropriate backups are taken at regular intervals and that such backups are retained securely. Backups should be sufficient in frequency to ensure that any potential loss of University Data requiring a ‘restore from backup’ is minimised (such that the loss is limited to 1 Business Day). The Consultant should ensure that both backup and restoration processes are tested at regular intervals to ensure their veracity, effectiveness, adequacy and appropriateness.

### **7.4  Logging and monitoring**

The Consultant should ensure that all system user and administrator/operator activities, exceptions, faults and information security events are accurately logged and protected.  Clocks should be synchronised in order to ensure accurate reliable records.

### **7.5  Control of operational software**

Software installation on operational systems and the Equipment should be controlled and Personnel and other end users should not be able to install unauthorised software within the ICT infrastructure or directly onto any of the Equipment.

### **7.6  Technical vulnerability management**

**7.6.1** It is the Consultant’s responsibility to identify, monitor and remedy any technical vulnerability in its ICT systems, the Equipment and any software used in the provision of the services or storage or Processing of the University Data. The Consultant should ensure that all technical vulnerabilities identified are patched and all systems kept up-to-date.

**7.6.2** The Consultant should put in place appropriate and effective rules governing software installation or configuration changes by Personnel and/or other users.

### **7.7  Information systems audit considerations**

The Consultant should ensure that IT audits are conducted at regular intervals, and that they are planned and controlled to minimise any adverse effects on the provision of services or production systems, and to minimise any risk of inappropriate data access.

1. **COMMUNICATIONS SECURITY**
   1. **Network security management**

The Consultant should ensure that all networks and network services are secured as appropriate, for example by way of network segregation where appropriate.

* 1. **Information transfer**

The Consultant shall ensure that appropriate policies, procedures and Contracts (*e.g.* non-disclosure Contracts) are in place concerning information and University Data transfer to/from Third Parties and in the case of information which is not University Data, any other third party, including policies, procedure and Contracts to govern the use of electronic messaging.

1. **SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE**
   1. **Security requirements of information systems**

The Consultant shall develop and put in place appropriate security control requirements, including requirements to govern web applications and transactions.

* 1. **Security in development and support processes**

The Consultant shall put in place appropriate rules to govern the development of secure software and systems development.  Changes to systems (both applications and operating systems) should be controlled and documented.  Software packages should be modified only in exceptional circumstances, and secure system engineering principles should be followed.  The Consultant is responsible for ensuring the development environment is secure, and that any outsourced development is properly vetted and controlled.  System security should be tested and acceptance criteria defined to include all appropriate security aspects.

* 1. **Test data**

### The Consultant shall ensure that all test data is carefully selected/generated, controlled and anonymised wherever possible.

### **THE CONSULTANT’S RELATIONSHIPS**

### **Information security in the Consultant’s relationships**

The Consultant shall ensure that there are policies, procedures, awareness *etc.* in place to protect the Consultant’s information and the University’s Data that is accessible to Third Parties and, in respect of information and/or data not relating to the University of the Service(s) that is accessible to other IT outsourcers and externals throughout the supply chain. These policies, procedures, awareness *etc* should be referenced and agreed within the contracts or Contracts with the Third Parties and/or other IT outsourcers and externals as appropriate.

* 1. **The Consultant’s service delivery management**

Service delivery by Third Parties and, in respect of service delivery not related to the services, other external parties should be monitored, and regularly reviewed/audited against the Contract, such other contracts and Contracts as may be in place and the Data Protection Laws.  Service changes should be appropriately controlled.

1. **INFORMATION SECURITY INCIDENT MANAGEMENT**
   1. **Management of information security incidents and improvements**

There should be established responsibilities and procedures to manage (report, assess, respond to and learn from) any Data Breach and or other information security events or incidents and any weaknesses identified should be consistently and effectively remedied.

1. **INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT**
   1. **Information security continuity**

The Consultant should ensure that the continuity of information security, particularly in relation to University Data, is planned, implemented and reviewed as an integral part of the Consultant’s business continuity management systems.

* 1. **Redundancies**

The Consultant shall ensure that the Equipment and all other IT facilities have sufficient capacity redundancy built in to satisfy availability requirements.

1. **COMPLIANCE**
   1. **Compliance with legal and contractual requirements**

The Consultant must identify, document and comply with its obligations to external authorities, regulatory bodies and other Third Parties in relation to information security, including intellectual property, business records, privacy/personally identifiable information and cryptography.

* 1. **Information security reviews**

The Consultant’s information security arrangements should be independently reviewed (audited) and reported to its management.  The Consultant’s management are required to routinely review Personnel, Equipment, system’s compliance with security policies, procedures *etc.,* and shall initiate and pursue all required corrective actions where necessary.

Appendix 2 - Schedule of Data

Categories of Data Subjects (tick as appropriate)

|  |  |
| --- | --- |
| University Employees |  |
| Students |  |

Personal data (tick as appropriate)

|  |  |
| --- | --- |
| **Date joined the University** |  |
| **First name** |  |
| **Last name** |  |
| **Email** |  |
| **Graduation year** |  |
| **Field of study** |  |
| **Degree** |  |
| **Clubs and honours** |  |
| **Address** |  |
| **Post Code** |  |
| **Phone number** |  |

**Special Category Data (Tick all that apply)**

|  |  |
| --- | --- |
| **Racial or ethnic origin** |  |
| **Political opinions** |  |
| **Religious/philosophical beliefs** |  |
| **Trade union membership** |  |
| **State of health** |  |
| **Criminal convictions** |  |