Schedule Z - Data Protection

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

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

|  |
| --- |
| **“Agreement”** means the main Agreement entered into between UOL and the Supplier dated [ ] . |
| **“Back-Up Policy”** means the policy and procedures that mitigate the risk of data loss, allow data to be restored, should an event such as data corruption, hardware failure or a security breach occur; |  |
| **“Controller”** has the meaning given to it in the Data Protection Laws; |
| **“Data Protection Authority”** means the Information Commissioner, or any other Regulatory Body responsible for enforcement of the Data Protection Laws from time to time in relation to UOL;  |
| **“Data Protection Laws”** means all applicable laws relating to the processing of Personal Data and privacy in force from time to time in the UK including, without limitation, the UK GDPR, the Data Protection Act 2018 and any regulations made thereunder, and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) and the guidance and codes of practice issued by the Data Protection Authority and which are applicable to a party; |
| **“Data Subject”** means any identified or identifiable individual to whom the Personal Data relates; |
| **"Law"** any applicable law, statute, bye-law, regulation, order, regulatory policy, guidance or industry code, rule of court or directives or requirements of any Regulatory Body, delegated or subordinate legislation or notice of any Regulatory Body; |
| **“Personal Data”** means any information relating to an identified or identifiable living individual that is processed by the Supplier on behalf of the UOL as a result of, or in connection with, the provision of the Services. An identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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; |
| **“Personnel”** means any person employed or engaged by or on behalf of Supplier who is engaged in the provision of the Services to the UoL and/or assists the Supplier with its performance of its obligations under the Agreement, including personnel employed or engaged by a Third-Party;  |
| **“Process” and other derivations such as “Processed” and “Processing”** means any activity that involves the 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. Processing also includes transferring the Personal Data to Third Parties; |
| **“Processor”** has the meanings given to it in the Data Protection Laws. |
| **"Regulatory Bodies"** means those government departments and regulatory, statutory and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this Contract; and "Regulatory Body" shall be construed accordingly; |
| **“Schedule”** means this Data Protection Schedule;“**Standard Contractual Clauses**” the ICO's International Data Transfer Agreement for the transfer of personal data from the UK and/or the ICO's International Data Transfer Addendum to EU Commission Standard Contractual Clauses and/or the European Commission's Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 as set out in the Annex to Commission Implementing Decision (EU) 2021/914 and/or the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU as adapted for the UK or such alternative clauses as may be approved by the European Commission or by the UK from time to time; |
| **“Third Party/Parties”** means any agent, supplier or sub-contractor or of the Supplier engaged by the Supplier in relation to the provision of the Services to UOL and/or who assists Supplier with its performance of its obligations under the Agreement in whole or part and who Processes Personal Data in doing so. |
| **“UK GDPR”** has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018. |
| **“UOL Data”** means all Personal Data belonging to UOL which is from time to time Processed under the Agreement by the Supplier and/or on the Supplier’s behalf including but not limited to all electronic data or information submitted by UOL and/or the users of UOL’s information technology systems and any Personal Data provided by or on behalf of UOL and any Personal Data in respect of any student or employees of UOL.  |
| **“Working Day”** means any day other than a Saturday, Sunday, bank holiday or public holiday in the City of London (UK) |

1. SUPPLIER AS DATA PROCESSOR
	1. In respect of the provision of the Services the parties agree and acknowledge:
		1. For the purposes of the Data Protection Laws, UOL is the Controller and the Supplier is a Processor in respect of UOL Data;
		2. Appendix 2 describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the Supplier may process the UOL Data.
		3. Where applicable to the Services being provided, the Supplier shall, at least annually for the duration of the Services and at the Supplier’s cost, undertake independent penetration testing using a CREST-accredited penetration tester. The Supplier must provide UOL with the penetration test summary.
		4. Where applicable to the Services being provided, the Supplier must maintain the security standard/accreditation agreed between the parties as part of the service provision, e.g., Cyber Essentials; Cyber Essentials+; ISO27001; Soc 2. The accreditation must be provided for the duration of the Services and the Supplier must provide UOL with evidence of renewal. Renewal must be completed either annually or at the frequency appropriate to the accreditation.
2. SUPPLIER’S OBLIGATIONS TO ACT ON INSTRUCTIONS
	1. Act on Instructions

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

* + 1. only Process UOL Data in order to provide the Services and then strictly only in accordance with the terms of the Agreement, this Schedule and such other written instructions received from UOL from time to time relating to UOL Data and shall not process UOL Data for any other purpose. The Supplier will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Laws. The Supplier must promptly notify the UOL if, in its opinion, UOL's instructions do not comply with the Data Protection Laws;
		2. promptly comply with any request from UOL requiring the Supplierto amend, transfer or delete any UOL Data or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing;
		3. promptly and fully cooperate with and assist UOL in relation to any reasonable request for cooperation and/or assistance and/or information relating to its Processing of UOL Data;
		4. at UOL’s request, promptly provide it with a copy of all UOL Data held by the Supplier in the format and on the media reasonably specified by UOL;
		5. keep full and proper records in accordance with the accountability requirements of the Data Protection Laws;
		6. ensure that UOL Data shall only be accessible by the Supplier’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 Agreement and who, where relevant, understand the confidentiality of such UOL Data and who are contractually bound to maintain its confidentiality.
		7. ensure that all Personnel are aware of the Supplier’s duties and their direct duties and obligations under the Data Protection Laws, this Schedule and the Agreement.
		8. not cause UOL 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 UOL Data except to the extent that the Supplier obtains the prior written consent of UOL and **PROVIDED ALWAYS** that the following conditions shall apply to such consent and after such consent is given:
			1. such Third Party shall not be entitled to sub-contract further in whole or in part or to allow any additional third party access to UOL Data;
			2. the Third Party’s appointment is otherwise on the same basis and terms as in this **clause 3** and the Supplier 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 UOL Data and the contract shall be provided to UOL and shall be subject to UOL’s express prior approval;
			3. the Supplier 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 UOL 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 UOL arising from any act or omission of any Third Party; and
			4. the Supplier shall comply with such other conditions as UOL may impose in relation to its consent from time to time.
	1. The Supplier shall follow its archiving procedures for UOL Data as set out in UOL’s Back-Up Policy (available on request from UOL), as such document may be amended by UOL in its sole discretion from time to time.
	2. If at any time the Supplier suspects or has reason to believe that any UOL Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Supplier shall notify UOL immediately and inform UOL of the remedial action it proposes to take.
	3. In addition to any other rights or remedies UOL may have, in the event of any loss or damage to UOL Data, the Supplier shall procure the restoration of the lost or damaged UOL Data from the latest back-up of such UOL Data maintained by it, or compensate UOL for so doing;
		1. the Supplier shall, in providing the Services, comply with UOL’s Privacy and Security Policy (available on request from UOL) as amended from time to time by UOL in its sole discretion; and
		2. the Supplier shall at all times in respect of Personal Data of which UOL is the Controller comply with obligations equivalent to those set out in the Data Protection Laws.
	4. **Security Measures**

The Supplier 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 processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and destruction or accidental loss, alteration, unauthorised disclosure or access to UOL Data (including, inter alia, (a) the pseudonymisation and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing; (e) 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 UOL 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 Agreement and the Data Protection Laws.
	1. **Data Breach**

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

* + 1. notify UOL 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 UOL Data or any other breach of security in relation to UOL Data or breach of any provision of the Data Protection Laws leading to the same (a “**Data Breach”**).
		2. thereafter provide UOL within 2 Working Days with all relevant information in its or their possession as required by UOL to comply with any informal or formal management and reporting obligations recommended or required by Data Protection Laws concerning any such Data Breach, including: nature or type of Personal Data or other information involved; categories and number of records involved/Data Subjects affected; circumstances of Data Breach; likely consequences of the 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 UOL of the content, media and timing of the Breach Notice (if any).
	1. **Treatment of Personal Data**

The Supplier 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 UOL Data and in particular shall ensure all UOL Data inputted or recorded is accurate and up to date (to the extent within the Supplier’s or Third Party’s control) and that such UOL Data is only retained in accordance with UOL’s data retention policy (available on request from UOL).

* 1. **Audit**

Subject to UOL and its auditors or other appointed professionals entering into reasonable confidentiality obligations, the Supplier 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 UOL, on reasonable notice and during regular business hours and at no cost to UOL:

* + 1. ensure that its and/or their staff, employees, directors, agents and other Personnel are made available to UOL 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 UOL Data and/or the performance of its obligations under this Schedule together with all premises where UOL 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 UOL;
		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 UOL 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 UOL to permit an accurate and complete assessment of the Supplier’s compliance with its obligations under this Schedule.

1. **REQUESTS FROM DATA SUBJECTS AND REGULATOR(S)**
	1. The Supplier warrants and undertakes that it shall, and shall procure that all Third Parties shall, notify UOL within two (2) Business Days, at no cost to UOL, 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 Laws, or of any other communication relating directly or indirectly to the Processing of any UOL Data in connection with this Agreement and provide all details of such complaint, request or communication to UOL and promptly and fully cooperate and assist UOL in relation to any such request or communication.
	2. Neither the Supplier 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 UOL Data, in each case unless expressly approved in writing in advance by UOL.
2. DATA TRANSFERS
	1. Subject to the terms of this Agreement the Supplier 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 UOL Data to be Processed or transferred outside the area consisting of the United Kingdom and the European Economic Area (together, the “**Permitted Territories**”) without the prior written consent of UOL and shall comply with the conditions imposed on such consent by UOL as set out in **clause 5.2**.
	2. The Supplier warrants and undertakes on a continuing basis that should it obtain the prior written consent referred to in **clause 5.1** prior to any Processing of UOL Data outside the Permitted Territories and/or to any transfer of UOL Data outside the Permitted Territories:
		1. Where the Supplier wishes to use a Third Party outside the Permitted Territories or who will Process UOL Data outside of the Permitted Territories, the Supplier 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 the Standard Contractual Clauses with UOL and the Supplier, at no additional cost to UOL and to include such terms as UOL shall, in its sole discretion, deem reasonable, appropriate or necessary;
		2. it shall provide a copy of each such executed Standard Contractual Clauses to UOL in advance of any such transfer.
		3. the Supplier shall procure the compliance of such Third Parties with the terms of the relevant Standard Contractual Clauses.
		4. The Supplier shall at all times remain responsible for the acts and omissions of the Third Parties in relation to UOL Data.
3. CONSEQUENCES OF EXPIRY AND TERMINATION
	1. The Supplier will liaise with UOL in the 3 month period prior to any termination or expiry of the Agreement to ascertain UOL’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 UOL Data (or, the secure deletion or destruction of all or part of UOL Data). If it is not possible for this to be carried out prior to termination or expiry, the Supplier shall cooperate with UOL about such preference and requirements as soon as possible on termination or expiry.
	2. The Supplier shall fully cooperate and comply with the preferences and requirements of UOL pursuant to **clause 6.1**. The Supplier shall also procure that Third Parties fully comply with these preferences and requirements.
	3. Subject to **clause 6.4**, the parties agree that:
		1. any deletion or destruction of UOL Data pursuant to **clause 6.1** shall be permanent and shall secure deletion of all requested UOL 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 UOL Data pursuant to **clause 6.1** shall be the secure return (as required by UOL) of all requested UOL Data in both electronic and hard copy formats (in whole or in part); and
		3. The Supplier shall certify in writing to UOL that it has complied with **clauses 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 UOL following termination or expiry of the Agreement.
	4. If the Supplier is required by Law to retain UOL Data post termination or expiry and cannot return or destroy it in accordance with **clause 6.1**, it shall
		1. immediately notify UOL in writing of the relevant UOL Data and the reason it must be retained and the required period of retention;
		2. be entitled to retain a single copy of such UOL Data;
		3. observe all the requirements of Data Protection Laws in relation to such UOL Data that is retained;
		4. only Process such UOL Data in accordance with the specific purposes and for the specific period for which the Supplier is under a legal duty to retain it;
		5. at the end of such period, securely and promptly destroy UOL Data within 7 days and certify to UOL in writing that it has done so; and
		6. promptly upon request provide to UOL such information as is reasonably necessary to enable UOL to satisfy itself of compliance by the Supplier and all Third Parties with this **clause 6**.

This **clause** shall continue in effect following termination or expiry of this Agreement.

1. **INDEMNITY**
	1. The Supplier shall, at all times during and after the termination or expiry of this Agreement, indemnify UOL, keep UOL indemnified and hold UOL 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 UOL arising from any breach of the Supplier’s obligations under this Schedule.
	2. Notwithstanding any other provision of this Schedule or the Agreement, Supplier’s liability under the indemnity at **clause 7.1** shall not be subject to any exclusions or limitations of liability.
	3. The Supplier shall take out insurance sufficient to cover any payment that may be required under this clause 7 and produce the policy and receipt for premium paid, to UOL on request.
2. **TRAINING**
	1. The Supplier will ensure that all Personnel are appropriately trained to Process Personal Data at all times;
	2. The Supplier 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 Supplier 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 Supplier 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**
	1. **Prior to employment**

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

#### **During employment**

#### The Supplier will ensure that all Personnel, employees and Suppliers are appropriately trained in relation to their and the Supplier’s obligations under the Data Protection Laws and are made aware of and motivated to comply with their information security obligations under this Agreement.  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 UOL 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 Supplier will ensure data security aspects of an employee’s exit or significant changes of roles are managed. The Supplier will ensure exiting employees and Personnel:

1. return all corporate information;
2. return all corporate equipment;
3. update access rights;
4. are made aware of their ongoing obligations under the Data Protection Laws, and their contractual terms.
5. **ASSET MANAGEMENT**
	1. **Responsibility for assets**
		1. The Supplier will ensure that all information assets including but not limited to UOL Data are inventoried and those with custody, control or responsibility for those assets, are identified and held clearly accountable for their security.
		2. The Supplier 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 UOL Data and all devices on which UOL Data has been stored or Processed are returned when Personnel leave employment or engagement of the Supplier or any Third Party.
	2. **Information Classification**

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

* 1. **Media handling**

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

### **ACCESS CONTROL**

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

The Supplier’s requirements to control access to information assets and UOL 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 UOL Data.

* 1. **Internal user access management**

The allocation of internal access rights to Personnel and in relation to other services not connected with the Services, 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 clause 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**

###  **Pseudonymisation**

### The Supplier shall implement such measures to ensure a level of security appropriate to the risk involved, including, as appropriate, the pseudonymisation of Personal Data.

### **Cryptographic controls**

The Supplier 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**
	1. **6.1  Secure areas**

The Supplier 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 UOL Data are stored or Processed*,* against unauthorised access.  The Supplier 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.*

#### **Equipment security**

* + 1. For the purposes of this Appendix 1 “**Equipment**” shall mean the ICT equipment, storage media and any other physical equipment used for the Processing or storage of UOL Data plus supporting utilities, (such as power and air conditioning) and cabling.
		2. All Equipment should be secured and maintained. Equipment and UOL Data should not be taken off-site unless expressly authorised by the Supplier and must be adequately protected both on the site of the University and off-site.
		3. Any UOL Data contained on any Equipment must be securely destroyed prior to such Equipment being disposed of or re-used.
		4. Unattended Equipment must be secured.
1. **OPERATIONS MANAGEMENT**

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

The Supplier 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 processes. The Supplier 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 UOL 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  Back-up**

###  The Supplier shall put in place and operate a back-up policy for the protection of UOL Data and to ensure compliance with the Schedule. Such back-up policy should include, but not be limited to a requirement that appropriate back-ups are taken at regular intervals and that such back-ups are retained securely. Back-ups should be sufficient in frequency to ensure that any potential loss of UOL Data requiring a ‘restore from back-up’ is minimised (such that the loss is limited to one Working Day). The Supplier 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 Supplier 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 Supplier’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 UOL Data. The Supplier should ensure that all technical vulnerabilities identified are patched and all systems kept up-to-date.

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

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

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

###  **THE SUPPLIER’S RELATIONSHIPS**

### **Information security in the Supplier’s relationships.**

The Supplier shall ensure that there are policies, procedures, awareness *etc.* in place to protect the Supplier’s information and UOL’s Data that is accessible to Third Parties and, in respect of information and/or data not relating to UOL 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 Agreements with the Third Parties and/or other IT outsourcers and external suppliers and services providers as appropriate.

* 1. **The Supplier’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 Agreement, such other Agreements as may be in place between the Supplier and the Third Party and the Data Protection Laws.  Service changes should be appropriately controlled.

1. **INFORMATION SECURITY INCIDENT MANAGEMENT**

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

* 1. **Redundancies**

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

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

  The Supplier 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 Supplier’s information security arrangements should be independently reviewed (audited) and reported to its management.  The Supplier’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

Purposes

|  |  |
| --- | --- |
| Subject matter of processing: |  |
| Duration of Processing: |  |
| Nature of Processing: |  |
| Business Purposes: |  |
| Authorised Persons: |  |
| Approved Sub-Contractors: | *[List all approved Sub-Contractors.]* |

Categories of Data Subjects (tick as appropriate)

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

Types of Personal Data (tick as appropriate)

|  |  |
| --- | --- |
| **Date joined UOL** |  |
| **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** |  |
| **Genetic Data, Biometric Data, Sex Life or Sexual Orientation** |  |