



CONTRACT REFERENCE: <<SAMPLE>>

SUPPLY OF TALENT BANK SERVICES - CLIENT TERMS OF BUSINESS

1. DEFINITIONS

1.1. In this Agreement the following definitions apply:

“Agreement”	means this Agreement including all schedules and appendices.
“Appointed Partner” or “Business Partner” of “Member Institution”	means any third party approved by the Client to have access to the Talent Bank for the purposes of engaging and managing academic contractors and other staff/workers
“Assignment”	means any task, role, opportunity or timed event that is offered by the Client or its Appointed Partners
“Client” or “<<CLIENT NAME>>”	means <<CLIENT NAME AND ADDRESS>>
“Hiring Manager” or “Manager” or “User”	means any individual approved by the Client to use the service to hire, manage, engage or otherwise interact with the System and Service
“Keystone”	means Keystone Employment Group No.1 Limited at Parsonage Farm, Vale Road, Dover CT15 5DH
“Service(s)”	means the Services to be provided under this Agreement including as specified in Schedule A - Service Description and Specification and delivered in accordance with Schedule B – Service Level Agreement
“Service Fee”	means the Fees payable in accordance with clause 3 and as specified in Schedule C- Service fees
“Talent Bank”	means the original non-customised Talent Bank solution

“Client Talent Bank” or ‘System”	means the customised and configured Talent Bank internet service for the engagement and management of academic contractors and other occasional staff/workers as per the Service as defined in Schedule A - Service Description and Specification
“Worker” or “Candidate” or ‘Academic Contractor”	means any individual the Client wishes to be considered as candidates for offers of work or assignments via the Talent Bank

1.2. Unless the context requires, references in the singular include the plural and references to the masculine include the feminine and vice versa.

1.3. The headings contained in this Agreement are for convenience only and do not affect their interpretation.

2. THE CONTRACT AND TERMINATION

2.1. This Agreement constitutes the contract between Keystone and the Client for the provision of the Services and is deemed to be accepted by the Client upon signature of this Agreement..

2.2. This Agreement contains the entire agreement between the parties unless otherwise agreed in writing by the Managing Director of Keystone and a Director of the Client.

2.3. No variation or alteration to this Agreement shall be valid unless the details of such variation is agreed between an authorised representative of Keystone and an authorised representative of the Client and is set out in writing and a copy of the varied terms is given to the Client stating the date on or after which such varied terms shall apply.

2.4. This Agreement will commence on the date of last signature by the parties below (“Effective Date”) and automatically expire on the five year anniversary of the Effective Date (“initial term”) unless terminated as provided within this Agreement. Beyond this initial term the Agreement can be extended by a 12 months extension period no more than twice by mutual agreement of the parties.

2.5. Not Used.

2.6. The Client may terminate this agreement with immediate effect if Keystone materially fails to deliver, or becomes incapable of delivering, the Services in accordance with this Agreement including agreed Service Level Agreement (as detailed in SCHEDULE B - SERVICE LEVEL AGREEMENT) and such failure or incapacity cannot be remedied within 7 (seven) days of such failure or incapacity being reported.

2.7. Either Party may terminate this agreement with immediate effect by written notice to the other if the other becomes insolvent.

2.8. In the event that, on the termination of this Agreement, the Transfer of Undertakings (Protection of Employment) Regulations 2006 (the "TUPE Regulations") apply or are alleged to apply, Keystone shall provide full co-operation to the Client to identify any employees to whom the TUPE Regulations may apply and shall promptly provide any other information or documentation which may be reasonably requested by the Client.

2.9 All rights and obligations of the parties which by their nature are reasonably intended to survive such termination or expiration will survive termination or expiration of this Agreement.

THE SERVICES

2.10 To the extent that the Services consist of configuration and customisation of Talent Bank, Keystone shall comply with the Service Level Agreement in Schedule B.

2.11 Keystone shall provide the Services using all reasonable skill and care, in line with good industry practice.

2.12 Keystone shall ensure that it provides suitable numbers of staff to deliver the Services and that the staff providing the Services are suitably qualified.

3. CHARGES

3.1. The Client agrees to pay Keystone the applicable Service Fees as specified and at the intervals specified in SCHEDULE C - FEES. The Client agrees to pay VAT at the prevailing rate where applicable by law.

3.2. Keystone reserves the right to charge interest on any overdue amounts at the rate of 2% above the Bank of England base rate, from the due date until date of payment.

3.3 Keystone shall invoice Client [monthly in arrears]. Invoice shall include the Client's PO number, details of the Services provided and any other information as required by the Client. Each invoice shall be sent to <<ACCOUNTS EMAIL ADDRESS AT CLIENT>>

3.4 The Client shall pay the invoices within thirty days of receipt of such invoice.

4. PAYMENT OF THE WORKERS OR CANDIDATES

4.1. The Client, or its Business Partner has overall responsibility for paying the Workers and where appropriate, for the deduction and payment of National Insurance Contributions and PAYE Income Tax applicable to the Worker pursuant to sections 44-47 of the Income Tax (Earnings and Pensions) Act 2003.

4.2. The operational delivery of the responsibilities mentioned in 4.1 will be the sole responsibility of the Client or its Business Partner.

5. LIABILITY

5.1. The Client or its Business Partner accepts full responsibility for ensuring the suitability of any Workers or Candidate for any assignment or work.

5.2. Keystone is not liable for any loss, expense, damage or delay arising from any negligence, dishonesty, misconduct or lack of skill of any Candidate or Worker.

5.3. The Client and/or Business Partners accept responsibility where and to the extent applicable for ensuring the health and safety of any Candidate as part of an assignment and shall advise and brief the Candidate accordingly .

5.4. Neither party limits its liability for:

5.4.1. death or personal injury caused by its negligence, or that of its employees, agents or Subcontractors (as applicable); or

5.4.2. fraud or fraudulent misrepresentation by it or its employees

5.4.3 any liability that cannot be restricted or limited by law.

5.5 The Client shall not be liable for any indirect or consequential loss arising under this Agreement.

5.6 The Client's liability under this Agreement shall be limited to the fees paid to Keystone in the twelve months preceding the claim.

6. DISPUTE RESOLUTION

6.1. In the event of any dispute between the parties arising out of or in connection with this Agreement (save for issues relating to the SLA which will be dealt with in accordance with the SLA escalation procedure), including any question relating to its existence, validity or termination except for termination in the situations stated in clauses 2.6 and 2.7 (including but not limited to any dispute arising out of or in connection with the TUPE Regulations):

6.1.1. the parties shall first try in good faith to resolve the dispute by negotiation between appointed contacts of the Client and Keystone

6.1.2. if the dispute cannot be resolved in accordance with Clause 6.1.1 within ten (10) business days of it first being notified in writing to the applicable appointed contacts, then the parties will try in good faith to resolve the dispute by negotiation between the Client's Director (or appointed authority) and the Managing Director (or appointed authority) of Keystone.

6.1.3. If the dispute remains unresolved for a further period of ten (10) business days after reference to the Client's Director and the Managing Director of Keystone in accordance with Clause 6.1.2 above, the parties will attempt to settle it by mediation. Unless otherwise agreed by the parties within ten (10) business days of a request to do so the mediator will be appointed from the Centre for Effective Dispute Resolution.

6.2. No party may commence or apply to join the other party into any court proceedings (except for a claim for injunctive relief) in relation to any such dispute until it has attempted to settle the dispute by mediation and either the mediation has failed or the other party has failed to participate in the mediation or the mediation has been ongoing for a period of 12 weeks from the initial mediation meeting and has not resulted in an agreed resolution.

7. CONFIDENTIALITY AND DATA

7.1. During the term of this Agreement and thereafter, each party will treat as confidential all information that they obtain concerning, but not limited to, the business, finances, technology and affairs of the other ("Confidential Information"). Each of the parties will use at least the same degree of care (and not less than a reasonable degree of care) it uses to prevent the disclosure of its own confidential information of like importance, to prevent the disclosure of Confidential Information of the other party. Each party will promptly notify the other party of any actual or suspected misuse or unauthorised disclosure of the other party's Confidential Information.

7.2. The provisions of this Clause 7 shall cease to apply to: (i) information that has come into the public domain other than by breach of this Clause or any other duty of confidence; (ii) information that is obtained from a third party without breach of this Clause or any other duty of confidence; and (iii) information that is required to be disclosed by a regulatory or government body or court of competent jurisdiction with power to compel the disclosure.

7.3. Each party will comply with its obligations pursuant to the Data Protection Legislation specifically, Keystone shall comply with its obligations in Schedule D and its obligations as a processor.

8. ASSIGNMENT AND SUBCONTRACTING

8.1. Subject to prior written consent of the Client, Keystone may assign, transfer, charge, sub-contract or deal in any other manner with all or any of its rights or obligations under this Agreement.

9. THIRD PARTIES

9.1. A person who is not a party to this Agreement shall not have any rights under or in connection with it.

10. FORCE MAJEURE

10.1. Neither party shall be liable to the other as a result of any delay or failure to perform its obligations under this Agreement if and to the extent such delay or failure is caused by an event or circumstance which is beyond the reasonable control of that party which by its nature could not have been foreseen by such a party or if it could have been foreseen was unavoidable. For the avoidance of doubt, this clause shall not excuse delays or failures to perform where the force majeure event consists of labour strikes or lock-outs by the employees of the affected party.

10.2 Where the force majeure event persists for a period of three months or longer, the unaffected party may terminate this Agreement immediately on written notice to the affected party.

11. NOTICES

11.1. Any notice or other communication required to be given to a party under or in connection with this Agreement shall be in writing and shall be delivered to the other party personally or sent by prepaid first-class post, recorded delivery or by commercial courier, at its registered office or sent by electronic mail to the other party's address set out below or as communicated in accordance with the provisions of this clause for such use:

Client: <<LEGAL EMAIL ADDRESS>> with a copy to <<Alternative email address>>

Keystone: <<Supplier contact email address>>

11.2. Any notice or communication shall be deemed to have been duly received if delivered personally, when left at the address referred to above or, if sent by prepaid first-class post or recorded delivery, at 9.00 am on the second business day after posting, or if delivered by commercial courier, on the date and at the time that the courier's delivery receipt is signed, or if sent by electronic mail to the correct address, on the next business day after transmission provided that the sender has not received a delivery failure notice, and has complied with any instructions in an out of office notice.

12. WAIVER AND CUMULATIVE REMEDIES

12.1. A waiver of any right under this Agreement is only effective if it is in writing and shall not be deemed to be a waiver of any subsequent breach or default. No failure or delay by a party in exercising any right or remedy under this Agreement or by law shall constitute a waiver of that or any other right or remedy, nor preclude or restrict its further exercise. No single or partial exercise of such right or remedy shall preclude or restrict the further exercise of that or any other right or remedy.

12.2. Unless specifically provided otherwise, rights arising under this Agreement are cumulative and do not exclude rights provided by law.

13. SEVERANCE

13.1. If a court or any other competent authority finds that any provision (or part of any provision) of this Agreement is invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed deleted, and the validity and enforceability of the other provisions of this Agreement shall not be affected.

13.2. If any invalid, unenforceable or illegal provision of this Agreement would be valid, enforceable and legal if some part of it were deleted, the provision shall apply with the minimum modification necessary to make it legal, valid and enforceable.

14. INTELLECTUAL PROPERTY

14.1 Both parties shall retain the intellectual property rights that existed and were registered prior to this agreement. This includes, but is not limited to logos, styles, branding, images and any other pre-existing marketing assets.

Any licence to the Client to use new intellectual property created as part of the provision of this service (such as front end website branding, functionality, service descriptions etc) shall terminate upon termination of this agreement and the Client shall hold no rights to transfer that created intellectual property to another service or product. Likewise, Keystone shall not re-use that Client specific intellectual property for another service. To the extent that such Client-specific intellectual property incorporates Client-owned intellectual property, Keystone shall delete or destroy such Client intellectual property promptly at the Client's sole discretion upon termination of this agreement.

14.2 Any URL, domain or other such facilities purchased by Keystone for use in the Service shall remain the property of Keystone unless transfer is agreed between both parties or if the Client purchases those assets or other facilities directly. Keystone hereby grants the Client a licence to use its applicable intellectual property rights in connection with the Services for the term of this Agreement.

14.3 The Client may not use the terminology 'Talent Bank' or '<<SERVICE NAME>>' or other derivatives to operate its own similar service which is a competitor to Keystone without the express consent of Keystone Employment Group. Keystone Talent Bank is a registered trade mark under no UK00003360798.

14.4 The Client hereby grants Keystone a non-sublicensable, revocable, royalty-free licence to use its name and logo strictly for the purpose of providing the Services under this Agreement. Such licence shall automatically terminate on expiry or earlier termination of this Agreement unless otherwise agreed between the parties.

15. LAW

15.1. This Agreement is governed by the law of England & Wales and are subject to the exclusive jurisdiction of the Courts of England & Wales.

15. INSURANCE

During the term of this Agreement and for a period of six years thereafter, Keystone shall procure, pay for and maintain (a) Employer's Liability Insurance of not less than £5 million, (b) Public Liability Insurance of not less than £5 million, and (c) Professional Indemnity Insurance (including cyber liability) of not less than £2 million. Keystone shall provide evidence of such insurance policies where requested by the Client.

SCHEDULE A - SERVICE DESCRIPTION AND SPECIFICATION

1.1 Summary Service Description

- 1.1.1 Keystone shall provide a web-based application (a customised and configured instance of its proprietary Talent Bank solution accessible from a dedicated website via all commonly used internet browsers and optimised for all main device types and accessed via a client specific domain, acquired, commissioned and maintained by Keystone.
- 1.1.2 Talent Bank will be available to authorised users only (as defined by the Client) and via approved authentication methods (minimum of Multi-Factor Authentication). For the avoidance of doubt there is no limit on the number of Client users permitted to access Talent Bank. Hiring managers (including those from approved affiliates and member institutions) HR teams and administrator-level users, candidates, contractors and other workers will all register, engage and use the functionality of the application via the same website.
- 1.1.3 The service will be securely hosted in Amazon Web Services (AWS) in line with the security and control requirements as detailed in the specification and managed by Keystone in accordance with its ISO9001 quality management systems and ISO27001 information security management standard and Cyber Essentials and in accordance with all legal and regulatory requirements and as per the Client's stated specification, requirements and governance.
- 1.1.4 The primary purpose of the Service is to provide an online solution for the engagement and management of academic contractors and other occasional staff for assignments of tasks, work and duties in accordance with the Client's desired requirements and policy.
- 1.1.5 The Service will manage allocation of assignments, pay and pay rates and the hours of work completed for Workers/Contractors (and other worker types as defined by the Client) with an output to a formatted timesheet file (or other methodology to be defined by the Client and agreed by Keystone and any other relevant third parties) for upload to the Client's own payroll system in order to remunerate the workers. The Client will maintain the status as the employer or/and the contracting body of all the workers, and where applicable accepts all responsibilities of an employer with regards to employment law, tax, national insurance, Home Office regulations and any other legal and regulatory requirements arising from the Client's status as the main contracting body and/or employer.
- 1.1.6 The Service will provide the processing requirements and applying the business rules and other specific functionality as described in 1.2 – Functional Specification

1.2 Summary of Preliminary Requirements – Basis for Service Specification

The Service shall be designed to deliver upon the below attached requirements, as stated by the Client. A number of the requirements are subject to clarification, confirmation and elaboration from the Client, along with some corresponding operational decisions to be made by the Client. Final revisions and alternations will be reflected in a specification to be signed off by the Client as part of implementation.

<<INCLUDE SUMMARY OF CLIENT USER REQUIREMENTS EITHER AS AN ATTACHMENT OR INSERTED TABLE>>

2. Implementation Plan and Milestones

Subject to the final implementation plan which shall be agreed between the parties by no later than 30 days following the Effective Date, Keystone shall meet the following milestone deadlines. Keystone shall not be in breach of this provision to the extent that a delay in meeting a milestone is caused by the Client's failure to provide timely input required for the applicable milestone to be completed on schedule.

- a. User Requirements gathering -
- b. Service Specification to be signed off by senior users -
- c. First iteration build work undertaken and presented for review -
- d. User changes and refinements taken on board -
- e. Second iteration presented with final changes gathered-
- f. Final version undergoes UAT- Sign off by senior users-
- g. User training and roll out plan agreed -
- h. First Member Institution/Cohorts engagement -
- i. Go Live of first cohorts –

SCHEDULE B - SERVICE LEVEL AGREEMENT

1. Service Description

Please refer to Schedule A- SERVICE DESCRIPTION AND SPECIFICATION

2. Support Commitments

In order to maintain clear communication channels and receive effective support, Client expects a defined support process, support team and contact details.

- Online during business hours Mon-Fri 0900-1700hrs excluding public holidays
- Online chat via embedded feature within the Talent Bank Application.
- Customer Support telephone and email support
- Escalation to Account Manager and Client Director as required
- Direct Account Manager mobile number contact for P1, P2 and Account Management support
- On site support for training and other activity as defined in the service description and as agreed with service owners

Out of hours support:

- Email for all P3 and P4 support issues
- Direct Account Manager mobile number for all P1 and P2 support issues
- Escalation to SMT as required

Keystone utilises a ticketing system for all queries and support, enabling users to track and audit all issues and queries.

2.1 Incident Management Service Level Agreement

All incidents and requests logged with support are to be given a priority (P1 – P5) and Keystone will work to achieve the response and resolution times detailed in the table below.

“Response time” is defined as the time it (the Service Provider i.e. Keystone) has to accept a “call” as genuine and requires investigation as an incident or to reject the call.

“Resolution time” is the time it takes from the initial placement of the call to when the “Incident” has been diagnosed, any underlying problem identified and it is resolved or a mutually agreed workaround is implemented.

Priority	Definition	Response SLA	Resolution SLA	Response Performance
P1	Showstopper, significant business or user impact	1 hour	4 Hours	95%
P2	High priority, impacting			95%

	effective use of the service for a significant number of users	2 hours	1 Business Day i.e. 8 hours	
P3	Normal priority, service impaired for a small number of users	4 hours	3 Business Days i.e. 24 hours	90%
P4	Low priority, service not functioning as expected, but not significantly affecting use	1 business Day i.e. 8 hours	5 Business Days i.e. 40 hours	90%
P5	Request – a non-service impacting requirement	1 business Day i.e. 8 hours	5 Business Days i.e. 40 hours	95%

2.2 Change Management

A request for change can be invoked as a result of an enhancement, service scope change, new service, preventative maintenance or corrective maintenance activity. Requests for change can be raised by either Keystone or Client and are to be logged as request for change calls with the Service Desk. Where Client logs the request for change call, the Service Desk is to promptly acknowledge that the call is logged however due to the potentially complicated nature of change there is no defined resolution time and it is accepted that there may be instances where the change is declined by Keystone.

Keystone is to ensure all requests for change are logged, evaluated, priced, signed-off and monitored with a further risk assessment if required. Keystone is to maintain the change records which are to be made available to Client on request (given reasonable notice).

All changes which involve additional charges, change to the scope or nature of the contract, that may impact service or user experience require sign off by Client, prior to the implementation of the change. Minor changes such as server patching which are not service or user impacting can remain within Keystone's internal change procedures and do not require authorisation from Client.

Emergency Change means an immediate change required to resolve an issue which is significantly affecting a service. In these circumstances, Client should still be informed prior to the implementation of the change. However if this is not feasible, then the change should go ahead and review of the change should be actioned after the event. Emergency Changes are still to be recorded etc.as per a change request by Keystone and the number of Emergency Changes monitored to ensure that the process is not being abused.

2.3 Escalation Procedure

Escalations can be initiated by both Keystone and Client where response or resolution times are not met, or unlikely to be met (proactive escalation).

Escalation will be based on the priority of the call as follows:

- i. **P1:** standard resolution time = 4hrs, escalate to Level 1 contact after 4hrs and Level 2 contact after 1 working day
- ii. **P2:** standard resolution time = 4hrs, escalate to Level 1 contact after 8hrs and Level 2 contact after 2 working days
- iii. **P3:** standard resolution time = 2 working days, escalate to Level 1 contact after 5 working days, and Level 2 contact after a further 5 working days
- iv. **P4:** standard resolution time = 4 Business Days, escalate to Level 1 contact after a further 6 working days and Level 2 contact after a further 6 working days

Level 1 contact: Client dedicated Account Manager<<INSERT CONTACT DETAILS>>

Level 2 contact: Client Director, Keystone <<INSERT CONTACT DETAILS>>

2.4 Complaints procedure

If Client is not satisfied with Keystone response or any other aspect of the Services, then a complaint may be raised. Complaints are to be reported to the Service Desk where they will be logged and referred to a member of Keystone's senior management team.

All complaints must be acknowledged as received within 4 working hours and a response issued within 2 working days. If the customer is still not satisfied with Keystone's response then the issue will be referred to the Dispute Resolution as per the contract.

3.0 Maintenance and Release management

3.1 Maintenance Window

Keystone operates a maintenance window between 1900hrs to 0500hrs Mon-Fri and from 1600hrs to 0600hrs Saturday to Sunday. During this period of time, the service may be either partially or wholly unavailable. Keystone will attempt where possible to provide at least five (5) days' notice of maintenance activities that will impact the service. Downtime during this time period shall not be included in availability calculations.

Keystone have the right to perform essential maintenance without notice if the service is deemed as a security risk.

3.2 Release Cycle

As software manufacturers release new versions or patches to supported software, Keystone will advise Client of the new releases and work with Client to implement them to a mutually agreed timetable. Software updates are to follow the Change Control Procedure as per above clause 2.3.

3.3 Critical Updates

Keystone may, at any time, decide to install a critical update for the purpose of improving security or for any other reason. As much notice as possible will be provided but any resulting outage will not contribute to calculations of unavailability according to the service levels defined in this Agreement. Keystone will promptly install any security patches as soon as they are available.

4.0 Security

Keystone as the host of the systems is responsible for ensuring both the physical and digital security of the systems and service. Keystone will follow industry standard best practice to secure and protect the service.

The Client Penetration Testing Policy will apply to all web facing services.

5.0 System Backups

The Client data on the servers managed by Keystone is backed up on a regular basis and retained as per the schedule below. These backups are performed to protect against critical server failure and are not seen as a method of restoring files accidentally deleted.

Data backup table:

Service	Cycle	Retention
Amazon EC2/RDS	Daily	30 days
Amazon s3 object storage	Daily	30 days (restoration available thereafter)

6.0 Disaster Recovery and Business Continuity

6.1 Scope

- Business Continuity/Disaster Recovery for general risks (as per risk register)
- Business Continuity/Disaster Recovery for Core Technical Services

6.2 General Risks

Keystone considers a number of risks to its business, operations and trading outside of core technical services. These are recorded and assessed as part of a Central Risk Register. This Business Continuity Policy and any procedures or processes arising from it shall apply to all such risks, other than those where any additional or individual policies may be applied. In addition a separate Information Asset Register and risk assessment is maintained and reviewed as part of Keystone's ISO27001 Information Management certification.

These risks and the responses to them include, but are not limited to:

- Risks to enterprise, trading, competition, sectors and markets
- Operational risks, such as denial of access, infrastructure, weather and travel disruption
- Extraordinary events, security incidents, civil unrest, disruption and Acts of God
- Third party and supplier disruption

6.3 Core Technical Services

By design, all Keystone core systems are hosted in 'the cloud' at secure data centres which completely eliminates any dependency, and therefore risk, on our internal hardware, network or data backup equipment.

Being cloud based also means neither we, or our customers and workers, are reliant on office space or facilities; all services can be accessed and operated from a standard web browser anywhere in the world.

The following systems and processes are covered by our cloud strategy:

- Talent Bank
 - Worker Profiles
 - Client Profiles
 - Assignment Details
 - Online Timesheets
 - Job Adverts
 - Reporting
 - Help & Support
- Opera III
 - Accounting Ledgers
 - Credit Control
 - Payroll / HMRC feeds (e.g. RTI)
 - Management Information
- Google Apps (Enterprise Edition)
 - Email, Chat, Video
 - All Documents
 - Intranets
- VoIP Phone System
 - All remote / home PCs have a 'softphone' configured with their normal DDI

6.4 Data Centre Redundancy for Hosted Services

All the above services are hosted on 'virtualised' infrastructure which provides underlying network and hardware redundancy across multiple sites. Amazon Web Services (AWS) is utilised for all core services including:

- 1) RDS / Database
- 2) EC2 (VM / Compute)
- 3) EFS (shared storage)
- 4) CloudFront (content delivery)
- 5) Route53 (domain management)
- 6) WAF (security)

6.5 Data Backup & Restoration

All backup services and data are incorporated into the AWS hosting services. Daily back ups take place and this data is retained for 90 days. Certain AWS S3 objects in data storage can be restored thereafter.

6.6 Departmental Business Continuity Plans

Members of Keystone's team regularly work from home each week with full access to systems and data. Each team also has a departmental plan for initiating and coordinating business continuity activities to cover different scenarios where the offices are not accessible.

6.7 Major Incidents

In the event of a major incident we have a communication plan which alerts staff, Clients and workers and provides status updates via a dedicated web page. In certain scenarios, specific Client branches of Talent Bank will also be able to carry incident-specific messaging.

6.8 Incident Communication Plan

6.8.1 Internal Communications

During Office Hours:

- Standard fire drill procedure: Staff gather at nominated muster points, Manager or senior staff member conducts roll call and follows procedures in the Site Emergency Binder and acts as lead contact for the emergency services if required.
- In consultation with emergency services, if applicable, the Manager or senior staff member instructs staff to return to the building or leave and go home (copies of BCP checklists handed out).
- If appropriate the Manager or senior staff member will contact staff not in the office or Next of Kin informing them of the incident and any relevant facts with instructions to stay away.
- Manager or senior staff member informs Managing Director, Operations Director and IT Manager of status once immediate safety issues have been attended to.

Outside Office Hours:

- Senior Manager informs Team BCP Coordinator to activate 'Out of hours cascade' procedure:
- Contacts managers of teams by phone and email advising them that the BCP has been activated and to stay at home and logon to the intranet / BCP section.
- Team managers repeat process to all direct reports.
- Senior Manager informs MD, Operations Director and IT Manager of incident and status.

Intranet BCP:

- Status page
 - Updates on affected site(s)
 - Updates on disruption to local roads and public transport
 - 'All-clear'
- Web links to:
 - Internal Contacts
 - Internal Systems / phones
- BCP checklist by department
- External Communication

6.8.2 External Communications

The external communication plan defines and prioritises the responsibilities for initiating and maintaining contact with:

- Customers
- Working Temporary Staff

- Not Working Temporary Staff
- Landlord
- Insurance company
- Key suppliers

All media enquiries are directed to the Managing Director.

7.0 Service Availability

The service will be accessible twenty-four (24) hours a day, seven (7) days a week, with a 99.9% targeted uptime for core operating hours of Mon-Fri 0900-1700hrs, excluding public holidays. 99.9% uptime means that for 99.9% of the core operating hours during any calendar month. Unavailability is a condition in which the service cannot be accessed, excluding during the planned maintenance window. Each instance of unavailability is a Service Outage.

If a Service Outage occurs, Keystone will notify the Client's Service Account Manager via email. This notice will include the reason for the Service Outage and the estimated time for restoration of the service if Keystone knows this information when it gives this notice. Keystone will also notify the Client's Service Account Manager via e-mail once the Service Outage is over and the Service is restored.

Availability calculation formula:

Availability = Uptime ÷ (Uptime + downtime)

Eg: 200 hrs availability per month (8hrs per day for 25 days)

2hrs of downtime is recorded in that period

Formula= 200 ÷ (200+2) = 0.99

Availability +99%

8.0 Service Reporting

Monthly Reporting

Keystone will provide CLIENT with one report per quarter (3 months). That report will include the following information for the previous three (3) months:

- **Management Summary;**
- **Service Summary** - a narrative summary of the service bringing out major changes, opportunities, achievements, areas for improvement and performance;
- **Service Levels and Targets** - a presentation of the major service levels showing volumes and performance against target including:
 - **Incident Analysis** - summaries of incidents arising:
 - Number of incidents
 - Resolution within SLA
 - Average incident resolution effort (hours)
- **Security** - a summary of any security incidents such as attempted breaches, virus detection's or similar;
- **Customer Complaints** – details of any complaints received and the response, including number of escalations and analysis of the complaints.

8.1 Service Metrics

The following Key Performance Indicators (KPIs) are to be included in the monthly report.

KPI	Measurement	Metric
Incident Resolution within SLA	Percentage of Service Desks calls resolved within SLA (by priority level)	95%
Service Availability	Uptime (excluding scheduled maintenance)	99.9%

SCHEDULE C- FEES

1.1 Implementation Fees

Included	Fee
Purchase of domain(s) Website front end build Hosting and server commissioning Customisation works Full functional build as per the requirements in SCHEDULE A- Service Description and Specification Iterations with user team Creation of frameworks and workplans and Worker Groups Integrations/exports as stated in the requirements Functionality to timesheet output file Project management and implementation 14 days of on site deployment and training Communications and marketing support for launch	£ Based on the requirements as described in Schedule A- Service Description and Specification

Implementation fees are payable in advance within 30 days of contract signature.

1.2 Annual licence fees

Annual Licence to use	Fee
All website domain and hosting costs All relevant certification and licensing costs Unlimited number of worker users Unlimited number of Manager users Unlimited number of Admin users Any additional hosting/server costs arising from service growth/expansion Mon-Fri 0900-1700 unlimited email, chat and telephone support from full UK customer support team Comms and marketing of service as required 14 days per annum of on site, in-person training and support Dedicated Account Manager- with direct and immediate POC Reporting and Management Information Suite as per Client specifications delivered monthly All relevant supporting financial reports/ledger data as per the specification Software updates to accommodate legislative or regulatory changes (ie changes to HMRC, DWP or statutory legislation requirements) Software updates to resolve bugs, errors or patches	£

Annual licence fees shall be paid monthly in arrears via 12 equal instalments.

1.3 Additional Services

Excluded from the annual licence fee is any additional development work or new functional modules for additional customisation or functionality, customer-requested enhancements or changes, cosmetic enhancements and other application changes not included in the original specification. These will be agreed on a case by case basis.

Additional Services	Fees
Billable development work for features and functionality outside of the Service Specification detailed in Schedule A	£ xxx per day (Day being an 8hr period Mon-Fri in normal working times and excluding public holidays) Minimum charge is one day. Bodies of work will always be compiled into a full fixed-fee quotation and guaranteed to be delivered at that flat rate, based on estimated days.
Additional Training Days	£xxx per day (day being Mon-Fri 0900-1700 in normal working times, excluding public holidays). This is for one person to provide additional on-site training days at the Client's London based campuses only over and above the 14 days per annum included in the annual license fee.

SCHEDULE D – DATA PROCESSING SCHEDULE

AGREEMENT

BETWEEN:-

(1) <<**CLIENT NAME AND ADDRESS**>> (the "Data Controller"); and

(2) **KEYSTONE EMPLOYMENT GROUP No.1 Limited**, of Parsonage Farm, Vale Road, Dover CT15 5DH (the "Data Processor").

BACKGROUND

This Agreement sets out the terms and conditions under which Personal Data, and Special Category Personal Data held by the named "Data Controller" will be processed by the named "Data Processor". The Parties enter into this Agreement to ensure compliance the Data Protection Legislation. The parties agree that all processing of Data must comply with the provisions of the Data Protection Legislation.

Paragraphs 11 and 12 Part II of Schedule 1 of the Data Protection Legislation place obligations on a Data Controller to ensure that any Data Processor it engages provides sufficient guarantees to ensure that the Processing of the Data carried out on its behalf will be secure. The Parties enter into this Agreement to ensure the protection and security of Data passed from the Data Controller to the Data Processor for Processing, or accessed by the Data Processor on the authority of the Data Controller for Processing, or otherwise received by the Data Processor for Processing on the Data Controller's behalf.

This Agreement further defines certain service levels to be applied to all Data related Services provided by the Data Processor.

IT IS AGREED

DEFINITIONS AND

INTERPRETATIONS In this Agreement:

"CLIENT" means <<**Client Name and Address**>>

"Data Protection Legislation" means any applicable law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to data protection and privacy, including General Data Protection Regulation ((EU) 2016/679) as incorporated into UK data protection law and as defined by the European Union (Withdrawal) Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ("UK GDPR"); the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated

by Directive 2009/136/EC), the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended, and, to the extent applicable, any other legislation relating to personal data and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data;

"Data" means any information of whatever nature that, by whatever means, is provided to the Data Processor by the Data Controller, is accessed by the Data Processor on the authority of the Data Controller or is otherwise received by the Data Processor on the Data Controller's behalf, for the purposes of the Processing specified in this Agreement, and shall include, without limitation, any Personal Data and/or Sensitive Personal Data;

"Data Subject", "Personal Data", "Special Category Data" and "Processing" shall have the same meanings as are assigned to those terms in the Data Protection Legislation;

"Data Breach" has the meaning in the Data Protection Legislation

"Services" means processing of the Data by the Data Processor in connection with and for the purposes of the provision of the services to be provided by the Data Processor to the Data Controller under this Agreement;

"Services Agreement" means the agreement for the provision of services between the Data Controller and the Data Processor identified in the Client Terms of Business for Supplying the Service.

"Parties" refers collectively to the parties to this Agreement, being Client and Keystone;

"The Purpose" Keystone, the Data Processor, provides a software service to operate the service. This will include providing: (1) a web-based portal that enables Client staff and Appointed Partners to identify, and offer assignments and opportunities to academic contractors (and other worker types) (2) suitable electronic records that record the key data associated with the academic contractors, their academic and work achievements and the assignments offered to them.

This will involve the web based collection of data on Contractors and Candidates who access and use the Service, as well as the assignments offered by the staff or Appointed Partners (including Member Institutions). The data is used for monitoring and managing the work assignments.

The Personal Data will be stored by the Data Processor within the European Economic Area (the "EEA").

1. APPLICATION OF THIS AGREEMENT

1.1 The Data Controller agrees to provide the Data Processor with the relevant Data required for the Purpose.

1.2 The information to be provided is as follows:

1.2.1 Candidate/Contractor details to enable the placement of individuals into assignments

1.2.2 Candidate/Contractor details to enable Client approved Users and approved partners (including Member Institutions) to pay Student/candidates for work completed

1.2.3 Candidate/Contractor details to enable reporting and Management Information provision (e.g. name and address, previous work history and experience, skills and academic history)

1.2.4 Candidate/Worker details to enable the monitoring and management of the service (e.g. assignment history, pay rate information and service monitoring information)

1.2.5 Any other information necessary for the fulfilment of the purpose.

1.3 For the avoidance of doubt the Data transferred to the Data Processor under the Agreement at no time becomes the property of the Data Processor.

1.4 In consideration of the obligations undertaken by the Data Processor in clauses 2-5 of this Agreement, below, the Data Controller agrees that it shall ensure that it complies at all times with the Data Protection Legislation and in particular, the Data Controller agrees that it shall ensure that any disclosure of Personal Data made by it to the Data Processor is made with the Data Subject's consent or is otherwise lawful.

2. DATA PROCESSING

2.1 The Data Processor is to act only on instructions from the Data Controller.

2.2 Data will be delivered to the Data Processor using the following procedures: Data will be collected by a secure user interface to be accessed through the World Wide Web by the Data Subject and Data Controller.

2.3 The Data Processor undertakes to:-

2.3.1 Process the Data at all times in accordance with the Data Protection Legislation and solely for the Purpose connected with provision by the Data Processor of the Services and in the manner specified from time to time by the Data Controller in writing and for no other purpose or in any manner except with the express prior written consent of the Data Controller;

2.3.2 Ensure that Personal Data will not be processed to support measures or decisions with respect to particular individuals;

2.3.3 Ensure that Personal Data will not be processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any Data Subject;

2.3.4 Ensure that the Data will not be disclosed to any third party without the prior written authority of the Data Controller.

2.4 No steps will be taken by the Data Processor to contact any party identified in the Data unless it is for the purposes of delivering the service set out in this contract or the Data Controller has given prior written consent.

2.5 All Personal Data held by the Data Processor including any archive or back-up copies, will be returned to the Data Controller and securely destroyed from any system that it is held on at a date to be agreed by the relevant parties. After this date, the Data Processor must promptly provide to the Data Controller a written declaration confirming that the Data has been returned and securely destroyed from its systems.

2.6 The Data Processor will not transfer, or permit the transfer of the Data, to any territory outside the EEA without the prior written consent of the Data Controller.

2.7 On reasonable notice, the Data Processor will allow its Data Processing facilities, procedures and documentation to be submitted for scrutiny by the Data Controller or its auditors in order to ascertain compliance with the relevant laws of the United Kingdom and the terms and conditions of this Agreement.

2.8 The Data Processor will ensure that each of its employees, agents and subcontractors are made aware of and comply with the obligations under this Agreement with regard to the security and protection of the Data.

2.9 In the event of the exercise by Data Subjects of any of their rights under the Data Protection Legislation in relation to the Data, the Data Processor will inform the Data Controller as soon as possible and in any event within 72 hours of any request by a Data Subject in respect of the exercise of their rights. The Data Processor agrees to assist the Data Controller with all Data Subject information requests which may be received from any Data Subject in relation to any Data.

2.10 In the event that the Data Processor receives a request for any information contained in the Data under the Freedom of Information Act 2000 the Data Processor will not respond to the person making such request but will inform the Data Controller within two (2) working days of its receipt. The Data Processor further agrees to assist the Data Controller with all such requests for information which may be received from any person within such timescales as may be prescribed by the Data Controller.

3. CONFIDENTIALITY

3.1 Under no circumstances will the Data Processor attempt to identify any person from the Data or aggregate data by any data matching or other exercise except where required for the Purpose.

4. SECURITY

4.1 The Data Processor agrees to apply appropriate security measures commensurate with the requirements of principle 7 of the Data Protection Act 2018. In particular, the Data Processor shall ensure at all times that adequate measures are in place to do everything possible to:-

- a. make accidental compromise or damage to the Data unlikely during storage, handling, use, Processing, transmission, transport or otherwise; and
- b. deter deliberate compromise or opportunist attack; and
- c. comply with the terms of Schedule D, Appendix 1 (Information Security).

4.2 The Data Processor shall ensure that security measures, commensurate with those operated by the Data Controller, shall be in force and applied at all times.

4.3 The Data Processor shall implement technological and all other reasonable measures to protect against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected.

4.4 Any security incidents, Data Breaches and newly-identified vulnerabilities must be reported to the Data Controller by the Data Processor immediately. In the case of any incident that gives rise to a Data Breach then the Data Processor shall inform the Data Controller promptly and in any case no later than within 24 hours of the Data breach occurring.

5. SUB- CONTRACTING

5.1 The Data Processor shall not sub-contract any of its rights or obligations under this Agreement without the prior written consent of the Data Controller.

5.2 Where the Data Processor, with the consent of the Data Controller, sub-contracts its obligations under this Agreement it shall do so only by way of a written agreement with the subcontractor which imposes the same obligations in relation to the security of the processing on the sub-contractor as are imposed on the Data Processor under this Agreement.

5.3 For the avoidance of doubt, where the subcontractor fails to fulfil its obligations under any sub-processing agreement, the Data Processor shall remain fully liable to the Data Controller for the fulfilment of its obligations under this Agreement.

5.4 Neither party shall assign or transfer any rights or obligations under this Agreement to another party without the prior written consent of the other.

6. RIGHTS OF THIRD PARTIES

6.1 Any rights, of any person, to enforce the terms of this Agreement pursuant to the Contracts (Rights of Third Parties) Act 1999 is hereby excluded.

7. TERMINATION

7.1 On expiry or termination of this agreement the Data Processor shall deliver to the Data Controller and/or securely destroy, at the Data Controller's sole option, all the Data Controller's Data in its possession or under its control.

8. INDEMNITY

8.1 The Data Processor is liable for and shall indemnify and keep the Data Controller fully indemnified on demand from and against each and every action, proceeding, liability, loss, damage, cost, claim, fine, expense and/or demand suffered or incurred by the Data Controller which arise from or in connection with or pursuant to any act or omission of or the performance of the Data Processor's obligations under this schedule, including without limitation those arising out of third party demand, claim or action, or any breach of contract, negligence, fraud, wilful misconduct, breach of statutory duty or non-compliance with this Agreement or any part of the Data Protection Legislation by the Data Processor or any of the Data Processor personnel.

Data Processing Particulars

The subject matter and duration of the processing	The parties will process Personal Data in the context of the applicable Services in this Agreement. Keystone shall process Personal Data on behalf of the Client as the Client's Processor on providing the Services contained in this Agreement. Keystone will process Personal Data for the duration of this Agreement. Personal Data will be retained in line with retention schedules of the Client and according to their direction to the Keystone.
The nature and purpose of the processing	The processing will be for the purposes of the provision of the Services.
The type of Personal Data being processed	The Personal Data will include: Workers details (ie date of birth, name, address, bank details), work assignment data (including timesheet

	and pay data) and payroll information (pay, NI tax code etc)
The categories of Data Subjects	The Data Subjects will include: Potential and actual workers who may be assigned work by the Client Staff of the Client. Staff of the Client's Member Institutions.

APPENDIX 1: INFORMATION SECURITY OBLIGATIONS

Keystone shall ensure that appropriate security measures including technical and organizational measures are in place at all times and backed up by robust policies and procedures to protect the Personal Data (copies to be provided to the University on request). Such measures shall include without limitation:

1. providing an appropriate level of information governance for all Personal Data;
2. ensuring that the hardware and software used in Processing the Personal Data are reliable and protected against all kinds of malicious software and viruses;
3. ensuring the methods of storing and Processing Personal Data provide sufficient security and control over access to the Personal taking account of the nature of the Personal Data;
4. using Multi-Factor Authentication on computer systems on which the Personal Data is stored;
5. taking reasonable steps to ensure the reliability of individuals who have access to the Personal Data, including but not limited to ensuring all such individuals understand the confidential nature of the Personal and the issues which arise if proper care is not taken in the use of the Personal Data and that all such individuals are properly trained in how to comply with Data Protection Legislation prior to accessing the Personal Data;
6. properly controlling remote access and ensuring that Personal Data is not downloaded to portable devices unless strictly necessary and only then if encrypted; and
7. ensuring a secure method for the deletion and disposal of Personal Data in whatever form.

DECLARATION

The Parties agree to abide by This Agreement. In doing so, the Parties are aware of and understand the relevant provisions of the Data Protection Legislation, and agree to abide by these provisions.

Authorised signature on behalf of <<CLIENT>>

Signature

Date

Print Name

Position

Authorised signature on behalf of **KEYSTONE EMPLOYMENT GROUP No.1 Ltd**

Signature

Date:

Print Name:

Position: