SCHEDULE 1

SERVICE LEVEL AGREEMENT

Case Priority Levels and Target Response Times.

Acolyte shall use a web-based support desk system to capture support incidents and keep Authorised Users informed at key moments of the support incident lifecycle.

Case Priority Level	Description	Target Response Time	Target Resolution Time
Critical	Major application component is down or otherwise unusable via the Application, which impacts ALL Users who are unable to use the Application in the Client's environment and there is no workaround. Web services module is down in production and is affecting major functionality within the Application.	Acolyte personnel will begin working the issue usually within 1 hour of receipt during Normal Business Hours.	4 Business Hours
High	Major application component is down or otherwise unusable via the Application, which impacts an individual User or subset of Users who are unable to use the Acolyte Application in Client's production environment.	Acolyte personnel will begin working the issue usually within 2 hours of receipt during Normal Business Hours.	8 Business Hours
Medium	Major application component is down or otherwise unusable via the Application and there is a workaround. Minor Application component is down or otherwise unusable, but it is not preventing the User from doing his/her job. Any issues defined as Critical or High in production are considered Medium in test environments (test, UAT, sandbox, development, etc.).	Acolyte personnel will usually begin working the issue within 2 hours of receipt during Normal Business Hours.	5 Business Days
Low	Cosmetic issues related to the Application. General Client questions.	Acolyte personnel will usually begin working the issue within 2 hours of receipt during Normal Business Hours.	10 Business Days

All cases will be prioritised according to the Case Priority Levels above. However, the Client may indicate the importance of their cases within the case priority levels noted above by providing an urgency rating as follows – Urgent, High, Standard. Once the Acolyte support representative has reviewed the case, the case may be re-classified with a different Case Priority Level. Feature requests and other initiatives are not assigned a priority but may be assigned an agreed upon due date.

Initial response times would be in relation to support hours of 9:00 am to 5:00 pm GMT Monday to Friday (Normal Business Hours), so that if an issue is reported outside of those hours the response will be within 1 or 2 hours, depending on 'Case Priority Level' from 09:00 GMT the next Business Day.

RESOLUTION TIMES

Acolyte has a maximum target resolution time by priority levels within the support coverage times, although, we aim to resolve issues much earlier. There are certain circumstances in which the monitoring and recording of resolution times might pause until certain criteria have been met, such as:

- The user has not clearly articulated the problem.
- If the diagnostic team cannot replicate the issue and need further information.
- Acolyte is awaiting a reply from an end user for clarification.

SCHEDULE 2

It is hereby agreed as follows:

This Arrangement lays down the distribution of responsibilities among the parties in connection with the parties being Joint Controllers for Candidate's personal data processed and shared between them under the Agreement.

1. Definitions

1.1. "Agreement" means Acolyte's Terms of Business.

1.2. **"Controller", "Processor", "Joint Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Processing" and "Technical and Organisational Measures"** have the meaning as set out in the GDPR.

1.3. **"Effective Date"** means the day when the Agreement is signed by the parties.

1.4. **"Candidate"** means any person who takes part in Acolyte's recruitment process as talent that may be suitable to fill the Client's vacancy.

1.5. **"Data Protection Legislation"** means all applicable data protection and privacy legislation in force from time to time in Europe, UK and any country where Candidates are based as relevant, including but not limited to, the GDPR, the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.

1.6. **"Permitted Recipients"** means the parties to the Agreement, the employees of each party, any third parties engaged to perform obligations in connection with the Agreement and this Arrangement and any professional advisors of either party.

1.7. **"Personal Data"** means the personal data that may be processed and shared as relevant between the parties under the Agreement. Personal Data shall be confined to the following categories of information relevant to the following categories of data subject:

Candidate's full name, LinkedIn profile, key skills, current job title, current job details, current company, company location, previous positions, job history, education, professional achievements, comments, reasons why they said 'no', CV, age, gender, ethnicity, sexual orientation and disability.

2. Compliance with the Data Protection Legislation

Each party will comply with (and shall ensure that its staff and/or subcontractors comply with) the Data Protection Legislation.

3. Transparency duties

3.1. Acolyte shall be responsible for giving full information to the Candidates whose Personal Data may be processed under the Agreement, pursuant to Articles 13 and 14 GDPR. Accordingly, Acolyte shall:

a) Create and publish the relevant privacy policies;

b) ensure that such privacy policies are written in clear and plain language and that provide sufficient information to the Candidates in order for them to understand what of their Personal Data is being processed as part of the recruitment process, the circumstances in which it will be processed, the purposes for the data Processing and either the identity with whom the data is shared or a description of the type of organisation that will receive the Personal Data, as well as how data subjects can exercise their requests pursuant to the rights granted by the GDPR and

c) ensure it has all necessary notices in place to enable lawful disclosure or transfer of the Personal Data to the Permitted Recipients in connection with the Agreement and this Arrangement.

3.2. Client shall also maintain its own privacy policy and notices as relevant.

4. Data subjects requests

4.1. Whereas data subjects may exercise the rights granted under the GDPR against any of the parties, each party shall be responsible for fulfilling the data subjects requests each party receives in connection with the Agreement and this Arrangement.

4.2. Each party shall provide the other party with reasonable assistance in complying with any data subject request each party may receive in connection with the Agreement.

5. General data protection principles

Each party shall comply with the data protection principles as set out in Article 5 GDPR. In particular, each party shall:

a) process Personal Data lawfully, fairly and in a transparent manner in relation to the Candidates;

b) collect Personal Data for specified, explicit and legitimate purposes and not further process it in a manner that is incompatible with those purposes;

c) process Personal Data in an adequate and relevant manner which shall be limited to what is necessary in relation to the purposes for which it is processed;

d) take any reasonable steps to ensure that Personal Data processed is accurate and kept up to date;

e) keep Personal Data in a form which permits identification of data subjects for no longer than is necessary for the performance of the Agreement;

f) process Personal Data in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate Technical and Organisational Measures.

6. Lawfulness of Processing

6.1. Each party shall have a lawful basis pursuant to Article 6 GDPR for Processing Personal Data processed and disclosed to the other party under the Agreement.

6.2. This Arrangement is made pursuant to Article 26 GDPR. Nothing contained in this Arrangement shall be construed to represent a substitution for the obligation of the parties to rely on a lawful Processing basis in compliance with Article 6 GDPR.

7. Security measures

Each party shall ensure that it has in place appropriate Technical and Organisational Measures to protect against unauthorised or unlawful Processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data including inter alia as appropriate:

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 and

d) a process for regularly testing, assessing and evaluating the effectiveness of Technical and Organisational Measures for ensuring the security of the Processing.

8. Notification of a Personal Data Breach to the supervisory authority and to the data subjects.

8.1. In the event of Personal Data Breach affecting Personal Data under the Agreement, the party who first identifies the data breach or the party from whom the reason for the breach originates shall inform the other party without undue delay and not later than 24 hours after having become aware of it.

8.2. The parties will jointly determine on a case by case basis whether the breach shall be notified to the competent supervisory authority and/or the affected data subjects.

8.3. Should the breach be reportable, the parties will jointly determine on a case by case basis which party notifies the breach to the competent supervisory authority and/or the affected data subjects.

9. Use of data Processors and sub-processors.

9.1. The parties are entitled to use data Processors and/or sub-processors in connection with the Agreement.

9.2. If any data Processors and/or sub-processors are used, each party is responsible for compliance with the requirements of Article 28 GDPR. The party using Processors and/or sub-processors shall, inter alia:

a) use only data Processors providing sufficient guarantees to implement appropriate Technical and Organisational Measures in such a manner that Processing will meet the requirements of the GDPR and ensure the protection of the Personal Data, rights and freedoms of the data subject and

b) ensure that a valid data Processing agreement has been made between the party as data Controller and the data Processor.

10. Transfers of data to third countries.

10.1. The parties may transfer Personal Data to third countries or international organisations where it is necessary for the performance of the Agreement.

10.2. At least one of the following safeguards shall be applied:

a) Standard Contractual Clauses adopted by the Commission or;

b) Binding Corporate Rules set out and approved in accordance with Article 47 GDPR.

10.3. Any transfer of data to third countries made on the basis of 10.2. shall be subject to a Data Transfer Impact Assessment whereby the parties confirm that:

a) the law in the recipient country ensures adequate protection for Personal Data transferred under the Agreement.

b) the data subject has enforceable rights and effective legal remedies.

10.4. Any mitigation measures identified pursuant to 10.3. shall be implemented as agreed by the parties.

10.5. A transfer of personal data to a third country or an international organisation may take place without any of the safeguards above where the Commission has decided that the third country ensures an adequate level of protection.

11. Organisation of contact with data subjects and supervisory authorities.

Either party may be contacted by the data subjects and supervisory authorities with regard to the provisions of this Arrangement. The parties will decide on a case by case basis how the matters for which they have been contacted shall be handled.