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

Acolyte will carry out processing of personal data in accordance with the Data Protection Act 1998, as amended and supplemented by the General Data Protection Regulation 2018, and the specific processes which shall be followed are set out below.

One – Personal data processing

The provision of services may entail the Processor's access to confidential information and personal data for which the Client is responsible. Consequently, Acolyte will be considered Data Processor, and any processing of personal data for which the Client is responsible will involve the different processes as agreed in the Agreement.

In order to render the services contained in this Agreement, the Client will make the Client Data, as applicable, available to Acolyte.

Two – Confidentiality and duty of secrecy

Unless the Parties otherwise agree, the Parties and all other companies belonging to its group or related thereto will keep the utmost secrecy of this Agreement, their business and any information and documentation related to the other Party, of which they may become aware as a result of performing the Agreement. Furthermore, the Processor hereby specifically undertakes to treat as confidential any information for which the Client or third parties may be responsible, which it may access due to providing its services, and undertakes to maintain the secrecy of such data.

For these purposes, the Processor hereby undertakes to take any measures that may be necessary, with respect to its employees or collaborators, in order for the latter to be informed of the need to fulfil its binding obligations as Processor and which, consequently, they must uphold, as well as to guarantee that any personal data known by virtue of this Agreement remain secret, even after the Agreement is terminated for any reason. To do this, the Processor will duly inform its employees or collaborators (through training, awareness campaigns, etc.), in order to ensure that such obligations are fulfilled. The foregoing will be comprehensibly notified of the existence of this Agreement, of any security rules affecting the development of their tasks, the consequences that may ensue in the event of breach and the confidential nature of such information and the duty to keep all personal data secret; this duty of confidentiality and secrecy will remain even after the relationship with the Processor has ended.

This duty of information and confidentiality on the part of the Processor's employees and collaborators will be carried out in such a way as to allow the Client to receive documentary evidence that such obligation has been fulfilled.

In addition, such confidential information and documentation may not be used for any purpose other than fulfilment of the object of this Agreement, unless such information has become general knowledge and except as regards any information required by law or further to any other applicable and mandatory regulations.

Once this Agreement has ended, the confidentiality obligation and duty of secrecy foreseen in this clause will remain valid indefinitely, even after the contractual relationship with the Controller has ended, for any reason.

If any misconduct is detected, by any person rendering professional services for the Processor (access to information not inherent to his tasks, misuse of user names and passwords, if a user is granted more authorisations that are strictly necessary, etc.), the Processor will be responsible and expressly obliged to immediately notify about it the Client, providing a detailed report of the facts.

Three – Controller's instructions

The Processor undertakes to process any personal data it may access exclusively in accordance with any written instructions provided by the Controller for this purpose. This commitment will also cover any international personal data transfers to a third country or international organisation.

Consequently, any data that is known or obtained by virtue of this Agreement:

- may not be used for any other purpose than performance thereof; they will be confidential and may not be published or made available to third parties without the Controller's prior written consent. In no case will such data be used privately.
- will not be notified to third parties without the Client's prior written consent. Consequently, the Processor, in writing and before the Client authorises such communication, will identify the entity(ies) receiving the data, which data or category of personal data will be reported and any security measures applicable.

In this regard, the Processor hereby undertakes to immediately inform the Controller if any of the latter's instructions could potentially infringe applicable provisions in data protection matters, under Community or Member State laws.

In the event that the Processor should use the data for another purpose, or reports or uses them in breach of the stipulations of this Agreement, it will also be considered data Controller, and will be personally liable for any infractions it may have incurred, as well as for any loss and damage that the Client may consequently suffer.

Four – Service outsourcing

The Processor will not outsource all or part of the services covered by this Agreement to another Processor, without the Controller's prior written consent, granted specifically or in general. The Controller hereby consents to the outsourcing of processing to Amazon Web Services EMEA SARL and Acolyte's development partner, NE6 Limited. The Processor will inform the Controller of any change foreseen in the hiring of new processors, or their replacement, thereby granting the latter the chance to challenge any such change.

If the Processor resorts to a sub-processor for the execution of certain processing activities on account of the Controller, always subject to the latter's prior authorisation, the sub-processor will be bound by the same data protection obligations stipulated for the Processor. The Processor will be fully liable vis-à-vis the Controller, and will be liable for effectively complying with data protection obligations on the part of such sub-processor.

Furthermore, the Processor undertakes to inform the Controller of any change foreseen in the hiring of new processors, or their replacement, sufficiently in advance (10 Business Days) and by authentic means, thus granting the Controller the chance to challenge such changes.

Five – Security measures

As of 25 May 2018, the Processor will be subject to security measures that are adequate to protect the personal data and other information, to be implemented by the Processor in accordance with the outcome of the risk evaluation completed by the Client, based on the state of the art, application costs, the nature of the data stored, the scope and purposes of the processing, and the risks to which they are exposed. Consequently, the Processor will provide the Client with the necessary information in those cases where its risk analysis indicates that the processing is high-risk, or if so is considered by the Processor.

The Processor will at least provide the Client with the following information, in writing (subject to availability):

- Any security measures implemented.
- Any other information that the UK Information Commissioner may request, held by the Processor.

In any case, the Processor will include the following measures as part of its technical and organisational measures.

Six – Notification of security breaches

The Processor will be obliged to guarantee implementation of the security requirements foreseen in this Agreement, and to inform the Client without undue delay of any incident affecting any information, documentation and personal data for which the Client is directly or indirectly responsible.

If the Processor or any person involved in the services were to detect an incident entailing data theft, loss or damage, if a person has had unauthorised access thereto, or if the information has been misused, the Processor will immediately get in touch with the Client, providing details of the incident and, in any case, within 40 hours of breach detection, by e-mail to the Client, attaching any relevant information to document and notify the incident, to include at least the following:

1. Description of the nature of the personal data security violation to include, whenever possible, the categories and approximate number of affected parties, and the categories and approximate number of personal data files affected.

2. The name and contact details of the data protection delegate or other contact point where more information may be obtained.
3. Description of any possible consequences.
4. Description of the measures adopted or proposed to remedy the personal data breach to include, if applicable, any measures to mitigate potential negative effects.

If it is not possible to provide the information simultaneously, and insofar as it is not simultaneous, information will be provided gradually and promptly.

The Processor will be responsible for taking any action that may be necessary to contain and resolve the incident.

The Client will conduct a periodic check on the current state of resolution of the incident; the Processor undertakes to respond and provide any reports that may be requested.

Seven – Record of processing categories

Starting on 25 May 2018 and only in those cases where the Processor has more than two hundred and fifty (250) employees or its processing entails a high risk for the rights of interested parties, or it is processing particularly sensitive data or related to convictions and criminal offences, it will keep a written record of all its processing categories, to include:

a. Contact details of both the Client and the Processor to include, as the case may be, of its representatives and data protection delegates.
b. The processing categories completed on behalf of the Client.
c. A general description of any technical and organisational measures applied.

Eight – Data subjects' rights

The Processor will assist the controller, by applying any appropriate technical and organisational measures and pursuant to the nature of the processed data, in relation to any requests to uphold the rights of interested parties, to particularly include their rights of access, rectification and cancellation (the "right to be forgotten"), and challenge to the processing of their data, a request for personal data portability, any processing limitations, as well as the right to not be the object of an automated individual decision, profiling included.

In the event that any data subject were to uphold the aforementioned rights vis-à-vis the Processor, the latter will duly notify the situation by e-mail to the Client. This notification must be made immediately and, in any case, no later than by the next business day following receipt of the request, along with any other information that may be relevant to attend the request.

Nine – Termination

At the end of the contractual service, the Processor undertakes to return any personal data and, as the case may be, any physical media containing the data, once the service is provided. This return will include a total erasure of all data existing in any computer equipment used by the Processor.

Furthermore, the Processor will guarantee that at the end of any contractual relationship held with any person carrying out professional duties:

- such person returns and does not withhold, in any way, the Client's information and resources.
- the foregoing is confirmed in a handwritten document or through any similar means permitted by current law.
- all authorisations to data processes are immediately cancelled.

Without prejudice to the foregoing, the Processor may keep a copy, with all data duly removed, insofar as it remains liable for performance of the services.

Ten – Audits

The Client, further to its controlling capacity, may carry out its own check-ups, in order to verify compliance with the security policies and measures required in this Agreement to protect personal information and data. These checks may be conducted on data systems and data processing facilities of the Processor, or may involve the gathering of information to corroborate the Processor's compliance. In any case, the Processor will keep documentation available to the Client (in printed or electronic form), confirming compliance with its obligations under the Agreement.

In order to facilitate or even avoid the Client's verification, the Processor may provide certifications, whose scope of application includes the services and staff offered by the latter to the Client. The foregoing will apply without prejudice to the possibility of completing any other audits or checks in order to verify other obligations foreseen in this Agreement.

Eleven – Duty of care

The Processor undertakes to provide to the Controller any information that may be necessary to evidence compliance with its obligations, and will inform the Processor in relation to its adhesion to an approved code of conduct, or its subscription of any certification system that is able to guarantee compliance with its personal data processing obligations.

Any persons carrying out professional tasks for the Processor must be aware of the importance of the Client's information, will process it safely and will be trained and qualified for each and every one of the data processing stages, for each and every task performed. Such persons will take the necessary care and will adopt adequate measures to protect the data processing, further to their contractually binding duty of good faith.

Twelve – Duty of information

The personal data of the Processor's representatives or contacts will, in turn, be processed by the Client, acting as the Controller, in order to manage the relationship held with the latter, as the Processor, based on the rendering of services; the controller has a legitimate interest in recording any phone conversations maintained between the parties and the data subject may as well exercise the rights of access, rectification, cancellation and challenge, may limit processing and portability, and may decide not to be the object of automated individualised decisions, by addressing the Data Protection Delegate at the foregoing address, referring to "DP" on the envelope, or by sending an e-mail to dataprotectionofficer@acolytegroup.co.uk. If intended, the data subject may as well file a claim before the data protection Authority.