Propeller powered

ANNIVERSARY 10 yrs

Workforce Management &
Compliance Solutions

Propeller

# Web-Hosted Hosted Services Agreement

# G-Cloud 15

Climate neutral
Company
ClimatePartner.com/14412-2008-1002

**HOSTED SERVICES AGREEMENT** made on [insert date]

**PARTIES**

**1.** …….. (the **Customer**); and

**2.** **PROPELLER POWERED LTD** a company incorporated in England and Wales (registration number 8301810) having its registered office at Unit 6 Mercury Way Urmston Manchester, M41 7LY (the **Provider**).

BACKGROUND

A. Upon execution, this agreement replaces and supersedes all previous agreements made between the parties relating to the subject matter hereof.

B. The Customer requires a job management and compliance reporting system to assist its carrying out of maintenance tasks to its clients.

C. The Provider has developed a job and compliance management reporting software to be provided as a web hosted service.

D. The Provider has agreed to provide hosting services to the Customer pursuant to the terms of this Agreement

**TERMS AND CONDITIONS**

**1. Definitions**

1.1 Except to the extent expressly provided otherwise, in these Terms and Conditions:

"**Account**" means an account enabling a person to access and use the Hosted Services, including both administrator accounts and user accounts;

"**Agreement**" means this contract, including the Services Order Form which is deemed incorporated herein, between the parties incorporating these Terms and Conditions, and any amendments to this contract from time to time;

"**Business Day**" means any weekday other than a bank or public holiday in England;

"**Business Hours**" means the hours of 09:00 to 17:00 GMT/BST on a Business Day;

"**Charges**" means the following amounts:

(a) the amounts specified in Section 3 of the Services Order Form;

(b) such amounts as may be agreed in writing by the parties from time to time;

"**Customer Confidential Information**" means:

any information disclosed by or on behalf of the Customer to the Provider at any time before the termination of the Agreement (whether disclosed in writing, orally or otherwise) that at the time of disclosure:

(i) was marked or described as "confidential"; or

(ii) should have been reasonably understood by the Provider to be confidential;

"**Customer Data**" means all data, works and materials: uploaded to or stored on the Platform by the Customer; transmitted by the Platform at the instigation of the Customer; supplied by the Customer to the Provider for uploading to, transmission by or storage on the Platform; or generated by the Platform as a result of the use of the Hosted Services by the Customer;

"**Customer Personal Data**" means any Personal Data that is processed by the Provider on behalf of the Customer in relation to the Agreement.

"**Data Protection Laws**" means all applicable laws relating to the processing of Personal Data including (but not limited to), while it is in force and applicable to Customer Personal Data, the UK retained General Data Protection Regulation (Regulation (EU) 2016/679) and the Data Protection Act 2018;

"**Documentation**" means the Hosted Services Specification included at Schedule 3 together with such other documentation for the Hosted Services produced by the Provider and delivered or made available by the Provider to the Customer;

"**Effective Date**" means the date upon which the Customer agrees contract and and submits the Services Order Form

"**Force Majeure Event**" means an event, or a series of related events, that is outside the reasonable control of the party affected (including failures of the internet or any public telecommunications network, hacker attacks, denial of service attacks, virus or other malicious software attacks or infections, power failures, industrial disputes affecting any third party, changes to the law, disasters, explosions, fires, floods, riots, terrorist attacks and wars);

**"Good Industry Practice"** means the standard of skill and care reasonably expected of a service provider in the Provider's industry

"**Hosted Services**" means the Propeller Powered Field Management and Compliance Software, which will be made available by the Provider to the Customer as a service via the internet in accordance with these Terms and Conditions;

"**Hosted Services Defect**" means a defect, error or bug in the Platform having a material adverse effect on the functionality or performance of the Hosted Services, but excluding any defect, error or bug caused by or arising as a result of:

(a) any negligent act or omission of the Customer or any person authorised by the Customer to use the Platform or Hosted Services;

(b) any use of the Platform or Hosted Services contrary to the Documentation, whether by the Customer or by any person authorised by the Customer;

(c) a failure of the Customer to perform or observe any of its obligations in the Agreement; and/or

(d) an incompatibility between the Platform or Hosted Services and any other system, network, application, program, hardware or software not specified as compatible in the Hosted Services Specification;

"**Hosted Services Specification**" means the specification for the Platform and Hosted Services set out in the Documentation;

"**Intellectual Property Rights**" means all intellectual property rights wherever in the world, whether registrable or unregistrable, registered or unregistered, including any application or right of application for such rights (and these "intellectual property rights" include copyright and related

rights, database rights, confidential information, trade secrets, know-how, business names, trade names, trade marks, service marks, passing off rights, unfair competition rights, patents, petty patents, utility models, semi-conductor topography rights and rights in designs);

"**Maintenance Services**" means the general maintenance of the Platform and Hosted Services, and the application of Updates and Upgrades.

**"Minimum Term"** means, in respect of this Agreement, the term of twelve (12) months beginning on the Effective Date;

"**Mobile App**" means the mobile application known as Propeller Powered that is made available by the Provider through the Google Play Store and the Apple App Store;

"**Personal Data**" has the meaning given to it in the UK retained General Data Protection Regulation (Regulation (EU) 2016/679);

"**Privacy Policy**" means the privacy and cookie policy which can be found at Privacy Policy;
"**Platform**" means the platform managed by the Provider and used by the Provider to provide the Hosted Services, including the application and database software for the Hosted Services, the system and server software used to provide the Hosted Services, and the computer hardware on which that application, database, system and server software is installed;

"**Services**" means any services that the Provider provides to the Customer, or has an obligation to provide to the Customer, under these Terms and Conditions;

**"Service Commitment"** means the commitment by the Provider to the availability of the Hosted Services to the Customer laid out in the Schedule 2(Service Level Agreement).

"**Services Order Form**" means an online order form published by the Provider and completed and submitted by the Customer, or a hard-copy order form signed or otherwise agreed by or on behalf of each party;

"**Support Services**" means support in relation to the use of, and the identification and resolution of errors in, the Hosted Services (as described in Schedule 2 hereto), but shall not include the provision of training services;

"**Supported Web Browser**" means the current release from time to time of Microsoft Edge, Mozilla Firefox, Google Chrome or Apple Safari;

"**Term**" means the term of the Agreement, commencing in accordance with Clause 2.1 and ending in accordance with Clause 2.2;

"**Terms and Conditions**" means all the documentation containing the provisions of the Agreement, namely the Services Order Form, these Terms and Conditions and Schedules and the Documentation including any amendments to that documentation from time to time made in accordance with these Terms and Conditions;

"**Update**" means a hotfix, patch or minor version update to any Platform software; and

"**Upgrade**" means a major version upgrade of any Platform software.

**2. Term**

2.1 The Agreement shall come into force upon the Effective Date.

2.2 The Agreement shall continue in force for the Minimum Term and thereafter on an annual rolling basis , subject to termination in accordance with Clause 17.

2.3 Not used.

**3. Hosted Services**

3.1 The Provider shall ensure that the Platform will, on the Effective Date, automatically generate an Account for the Customer and provide to the Customer login details for that Account.

3.2 The Provider hereby grants to the Customer a worldwide, non-exclusive licence to use the Hosted Services by means of a Supported Web Browser for the internal business purposes of the Customer in accordance with the Documentation during the Term.

3.3 The licence granted by the Provider to the Customer under Clause 3.2 is subject to the following limitations:

(a) the Hosted Services may only be used by the officers, employees, agents and subcontractors of the Customer;

(b) the Hosted Services must not be used at any point in time by more than the number of concurrent users specified in user list, providing that the Customer may add or remove concurrent user licences in accordance with the procedure set out herein.

3.4 Except to the extent expressly permitted in these Terms and Conditions or required by law on a non-excludable basis, the licence granted by the Provider to the Customer under Clause 3.2 is subject to the following prohibitions:

(a) the Customer must not sub-license its right to access and use the Hosted Services;

(b) the Customer must not permit any unauthorised person to access or use the Hosted Services;

(c) the Customer must not make any alteration to the Platform, except as permitted by the Documentation.

3.5 The Customer shall use reasonable endeavours, including reasonable security measures relating to administrator Account access details, to ensure that no unauthorised person may gain access to the Hosted Services using an administrator Account.

3.6 The Parties acknowledge that Schedule 2 (Service Level Agreement) shall govern the Service Commitment and the Provider shall use all reasonable endeavours to maintain the Service Commitment but does not guarantee 100% availability.

3.7 For the avoidance of doubt, downtime caused directly or indirectly by any of the following shall not be considered a breach of the Agreement:

(a) a Force Majeure Event;

(b) a fault or failure of the internet or any public telecommunications network;

(c) a fault or failure of the Customer's computer systems or networks;

(d) any breach by the Customer of the Agreement; or

(e) scheduled maintenance carried out in accordance with the Agreement.

3.8 The Customer must comply with Schedule 1 (Acceptable Use Policy), and must ensure that all persons using the Hosted Services with the authority of the Customer or by means of an administrator Account comply with Schedule 1 (Acceptable Use Policy).

3.9 The Customer must not use the Hosted Services in any way that causes, or may cause, damage to the Hosted Services or Platform or impairment of the availability or accessibility of the Hosted Services.

3.10 The Customer must not use the Hosted Services:

(a) in any way that is unlawful, illegal, fraudulent or harmful; or

(b) in connection with any unlawful, illegal, fraudulent or harmful purpose or activity.

3.11 For the avoidance of doubt, the Customer has no right to access the software code (including object code, intermediate code and source code) of the Platform, either during or after the Term.

3.12 The Provider may suspend the provision of the Hosted Services if any amount due to be paid by the Customer to the Provider under the Agreement is overdue. In such event the Provider will not be liable for any inconvenience loss or damage that the Subscriber or any other party may suffer including any consequential loss.

3.13 The Provider will provide the Hosted Services in accordance with Good Industry Practice.

3.14 The Provider warrants the Hosted Services will not introduce any virus, malware, Trojan and / or other malicious form(s) of software into the Customer's IT networks and environment and will use all reasonable endeavours, in accordance with Good Industry Practice, to ensure the same (including but not limited to the use of firewalls, anti-virus software, etc).

**4. Maintenance Services**

4.1 The Provider shall provide the Maintenance Services to the Customer during the Term. The Provider will endeavour to carry out any such maintenance during periods of minimal usage.

4.2 The Provider shall where practicable give to the Customer at least 14 Business Days' prior notice of scheduled Maintenance Services that are likely to affect the availability of the Hosted Services or are likely to have a material negative impact upon the Hosted Services, without prejudice to the Provider's other notice obligations under these Terms and Conditions.

4.3 The Provider shall give to the Customer at least 14 Business Days' prior notice of the application of an Upgrade to the Platform.

**5. Support Services**

5.1 The Provider shall provide the Support Services to the Customer during the Term.

5.2 The Provider shall make available to the Customer a helpdesk in accordance with the provisions of this main body of these Terms and Conditions.

5.3 The Provider shall provide the Support Services in accordance with Good Industry Practice.

5.4 The Customer may use the helpdesk for the purposes of requesting and, where applicable, receiving the Support Services; and the Customer must not use the helpdesk for any other purpose.

5.5 The Provider shall respond promptly to all requests for Support Services made by the Customer through the helpdesk.

5.6 The Provider may suspend the provision of the Support Services if any amount due to be paid

by the Customer to the Provider under the Agreement is overdue.

**6. Customer Data**

6.1 The Customer hereby grants to the Provider a non-exclusive licence to copy, reproduce, store, export, adapt, edit and translate the Customer Data to the extent reasonably required for the performance of the Provider's obligations and the exercise of the Provider's rights under the Agreement. Subject to clause 12.

6.2 The Customer warrants to the Provider that the Customer Data when used by the Provider in accordance with the Agreement will not infringe the Intellectual Property Rights or other legal rights of any person, and will not breach the provisions of any United Kingdom law, statute or regulation.

6.3 The Provider shall create a back-up copy of the Customer Data at least daily, shall ensure that each such copy is sufficient to enable the Provider to restore the Hosted Services to the state they were in at the time the back-up was taken, and shall retain and securely store each such copy for a minimum period of 30 days.

**7. Mobile App**

7.1 The parties acknowledge and agree that the use of the Mobile App, the parties' respective rights and obligations in relation to the Mobile App and any liabilities of either party arising out of the use of the Mobile App shall be subject to the terms and conditions of this Agreement.

**8. No assignment of Intellectual Property Rights**

8.1 Nothing in these Terms and Conditions shall operate to assign or transfer any Intellectual Property Rights from the Provider to the Customer, or from the Customer to the Provider.

**9. Charges**

9.1 The Customer shall pay the Charges to the Provider in accordance with these Terms and Conditions.

9.2 The payment schedule for the Customer is 100% on order of the Hosted Services, being due on 30 days from receipt of the Provider's invoice. Additional services days will be invoiced as taken.

9.3 All amounts stated in or in relation to these Terms and Conditions are, unless the context requires otherwise, stated exclusive of any applicable value added taxes, which will be added to those amounts and payable by the Customer to the Provider.

**10. Payments**

10.1 The Provider shall issue invoices for the Charges to the Customer on or after the invoicing dates.

10.2 The Customer must pay the Charges to the Provider, unless specified otherwise, within the period of 30 days following receipt of an invoice in accordance with this Clause 10.

10.3 The Customer must pay the Charges by direct debit or bank transfer using such payment details as are notified by the Provider to the Customer from time to time.

10.4 If the Customer does not pay any amount properly due to the Provider under these Terms and Conditions, the Provider may:

(a) charge the Customer interest on the overdue amount at the rate of 4% per annum above the Bank of England base rate from time to time (which interest will accrue daily until the date of actual payment and be compounded at the end of each calendar month); or

(b) not used

**11. Provider's confidentiality obligations**

11.1 The Provider must:

(a) keep the Customer Confidential Information strictly confidential;

(b) not disclose the Customer Confidential Information to any person without the Customer's prior written consent;

(c) use the same degree of care to protect the confidentiality of the Customer Confidential Information as the Provider uses to protect the Provider's own confidential information of a similar nature, being at least a reasonable degree of care;

(d) act in good faith at all times in relation to the Customer Confidential Information; and

11.2 Notwithstanding Clause 11.1, the Provider may disclose the Customer Confidential Information to the Provider's officers, employees, professional advisers, insurers, agents and subcontractors who have a need to access the Customer Confidential Information for the performance of their work with respect to the Agreement and who are bound by a written agreement or professional obligation to protect the confidentiality of the Customer Confidential Information.

11.3 This Clause 11 imposes no obligations upon the Provider with respect to Customer Confidential Information that:

(a) is known to the Provider before disclosure under these Terms and Conditions and is not subject to any other obligation of confidentiality;

(b) is or becomes publicly known through no act or default of the Provider.

11.4 The restrictions in this Clause 11 do not apply to the extent that any Customer Confidential Information is required to be disclosed by any law or regulation, by any judicial or governmental order or request, or pursuant to disclosure requirements relating to the listing of the stock of the Provider on any recognised stock exchange.

11.5 Within 5 days of the date of termination of this Agreement, the Provider must destroy or return to the Customer (at the Customer's option) all media containing the Customer Confidential Information and must irrevocably delete the Customer Confidential Information from its computer systems.

11.6 The provisions of this Clause 11 shall continue in force for a period of 5 years following the termination of the Agreement, at the end of which period they will cease to have effect.

**12. Data protection**

12.1 Each party shall comply with the Data Protection Laws with respect to the processing of the Customer Personal Data. The parties acknowledge that the Customer is the data controller and the Provider is the data processor of any personal data and the Provider shall comply with the Customer's instructions in relation to the processing of any personal data under this Agreement in accordance with Schedule 4.

12.2 The Customer warrants to the Provider that it has the legal right to disclose all Personal Data that it does in fact disclose to the Provider under or in connection with the Agreement.

12.3 The Provider shall only process the Customer Personal Data during the Term and for not more than 30 days following the end of the Term, subject to the other provisions of this Clause 12.

12.4 The Provider shall only process the Customer Personal Data on the documented instructions of the Customer (including with regard to transfers of the Customer Personal Data to any place outside the United Kingdom, as set out in these Terms and Conditions or any other document agreed by the parties in writing.

12.5 Notwithstanding any other provision of these Terms and Conditions, the Provider may process the Customer Personal Data if and to the extent that the Provider is required to do so by applicable law. In such a case, the Provider shall inform the Customer of the legal requirement before processing, unless that law prohibits such information.

12.6 The Provider shall ensure that persons authorised to process the Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

12.7 The Provider and the Customer shall each implement appropriate technical and organisational measures to ensure an appropriate level of security for the Customer Personal Data.

12.8 The Provider must not engage any third party to process the Customer Personal Data without the prior specific or general written authorisation of the Customer.

12.9 The Provider shall, insofar as possible and taking into account the nature of the processing, take appropriate technical and organisational measures to assist the Customer with the fulfilment of the Customer's obligation to respond to requests exercising a data subject's rights under the Data Protection Laws.

12.10 The Provider shall assist the Customer in ensuring compliance with the obligations relating to the security of processing of personal data, the notification of personal data breaches to the supervisory authority, the communication of personal data breaches to the data subject, data protection impact assessments and prior consultation in relation to high-risk processing under the Data Protection Laws.

12.10A The Provider must notify the Customer of any Personal Data breach affecting the Customer Personal Data without undue delay and in any event within 48 hours after the Provider becomes aware of the breach.

12.11 The Provider shall make available to the Customer all information necessary to demonstrate the compliance of the Provider with its obligations under this Clause 12 and the Data Protection Laws.

12.12 The Provider shall, at the choice of the Customer, delete or return all of the Customer Personal Data to the Customer after the provision of services relating to the processing, and shall delete existing copies save to the extent that applicable law requires storage of the relevant Personal Data.

12.13 The Provider shall allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer in respect of the compliance of the Provider's processing of Customer Personal Data with the Data Protection Laws and this Clause 12. The Provider may charge the Customer at its standard time-based charging rates for any work performed by the Provider at the request of the Customer pursuant to this Clause 12.14.

12.14 If any changes or prospective changes to the Data Protection Laws result or will result in one or both parties not complying with the Data Protection Laws in relation to processing of Personal Data carried out under these Terms and Conditions, then the parties shall use their best endeavours promptly to agree such variations to these Terms and Conditions as may be necessary to remedy such non-compliance.

**13. Warranties**

13.1 The Provider warrants to the Customer that:

(a) the Provider has the legal right and authority to enter into the Agreement and to perform its obligations under these Terms and Conditions;

(b) the Provider will comply with all applicable legal and regulatory requirements applying to the exercise of the Provider's rights and the fulfilment of the Provider's obligations under these Terms and Conditions; and

(c) the Provider has or has access to all necessary know-how, expertise and experience to perform its obligations under these Terms and Conditions.

13.2 Not used.

13.3 The Provider warrants to the Customer that the platform will incorporate security features reflecting the requirements of Good Industry Practice.

13.4 The Provider warrants to the Customer that the Hosted Services, when used by the Customer in accordance with these Terms and Conditions, will not breach any laws, statutes or regulations applicable under English law.

13.5 The Provider warrants to the Customer that the Hosted Services, when used by the Customer in accordance with these Terms and Conditions, will not infringe the Intellectual Property Rights of any person and the Provider indemnifies and holds harmless the Customer in respect of any alleged or actual claims, losses, costs and/or expenses, howsoever arising, incurred by the Customer as a result of the Hosted Services infringing the Intellectual Property Rights of any person.

13.6 The Customer warrants to the Provider that it has the legal right and authority to enter into the Agreement and to perform its obligations under these Terms and Conditions.

13.7 All of the parties' warranties and representations in respect of the subject matter of the Agreement are expressly set out in these Terms and Conditions. To the maximum extent permitted by applicable law, no other warranties or representations concerning the subject matter of the Agreement will be implied into the Agreement or any related contract.

**14. Acknowledgements and warranty limitations**

14.1 The Customer acknowledges that complex software is never wholly free from defects, errors and bugs; and subject to the other provisions of these Terms and Conditions, the Provider gives no warranty or representation that the Hosted Services will be wholly free from defects, errors and bugs.

14.2 The Customer acknowledges that complex software is never entirely free from security vulnerabilities; and subject to the other provisions of these Terms and Conditions (in particular clause 3.14), the Provider gives no warranty or representation that the Hosted Services will be entirely secure.

14.3 The Customer acknowledges that the Hosted Services are designed to be compatible only with that software and those systems specified as compatible in the Hosted Services Specification; and the Provider does not warrant or represent that the Hosted Services will be compatible with any other software or systems.

14.4 The Customer acknowledges that the Provider will not provide any legal, financial, accountancy or taxation advice under these Terms and Conditions or in relation to the Hosted

Services; and, except to the extent expressly provided otherwise in these Terms and Conditions, the Provider does not warrant or represent that the Hosted Services or the use of the Hosted Services by the Customer will not give rise to any legal liability on the part of the Customer or any other person.

**15. Limitations and exclusions of liability**

15.1 Nothing in these Terms and Conditions will:

(a) limit or exclude any liability for death or personal injury resulting from negligence;

(b) limit or exclude any liability for fraud or fraudulent misrepresentation;

(c) limit any liabilities in any way that is not permitted under applicable law; or

(d) exclude any liabilities that may not be excluded under applicable law.

15.2 The limitations and exclusions of liability set out in this Clause 15 and elsewhere in these Terms and Conditions:

(a) are subject to Clause 15.1; and

(b) govern all liabilities arising under these Terms and Conditions or relating to the subject matter of these Terms and Conditions, including liabilities arising in contract, in tort (including negligence) and for breach of statutory duty, except to the extent expressly provided otherwise in these Terms and Conditions.

15.3 Neither party shall be liable to the other in respect of any losses arising out of a Force Majeure Event.

15.4 Neither party shall be liable to the other in respect of any loss of profits or anticipated savings.

15.5 Neither party shall be liable to the other in respect of any loss of revenue or income.

15.6 Neither party shall be liable to the other in respect of any loss of use or production.

15.7 Neither party shall be liable to the other in respect of any loss of business, contracts or opportunities.

15.8 The Provider shall not be liable to the Customer in respect of any loss or corruption of any data, database or software; providing that this Clause 15.8 shall not protect the Provider unless the Provider has fully complied with its obligations under Clause 6.3.

15.9 Neither party shall be liable to the other in respect of any special, indirect or consequential loss or damage.

15.10 Subject to Clause 15.1, the Customer's liability to the Provider under or in connection with this Agreement, whether arising in contract, tort (including negligence), for breach of statutory duty, under any indemnity or however otherwise arising at law, shall be limited to a sum equal to 100% (one hundred per cent) of the Charges payable by the Customer, to the Provider, under this Agreement.

**16. Force Majeure Event**

16.1 If a Force Majeure Event gives rise to a failure or delay in either party performing any obligation under the Agreement (other than any obligation to make a payment), that obligation will be suspended for the duration of the Force Majeure Event.

16.2 A party that becomes aware of a Force Majeure Event which gives rise to, or which is likely to give rise to, any failure or delay in that party performing any obligation under the Agreement, must:

(a) promptly notify the other; and

(b) inform the other of the period for which it is estimated that such failure or delay will continue.

16.3 A party whose performance of its obligations under the Agreement is affected by a Force Majeure Event must take reasonable steps to mitigate the effects of the Force Majeure Event.

**17. Termination**

17.1 Following the expiration of the Minimum Term,

(a) the Customer may terminate this Agreement by giving to the provider at least 30 days written notice of termination;

(b) The Provider may terminate this Agreement by giving to the Customer at least 90 days written notice of termination

17.2 Either party may terminate the Agreement immediately by giving written notice of termination to the other party if the other party commits a material breach of these Terms and Conditions.

**18. Effects of termination**

18.1 Except to the extent that these Terms and Conditions expressly provides otherwise, the termination of the Agreement shall not affect the accrued rights of either party.

18.2 The parties acknowledge that the Customer will not incur any penalties by way of additional Charges or otherwise as a result of termination by either party in accordance with clause 17.1 or 17.2.

18.3 Within 90 days following the termination of the Agreement for any reason:

(a) the Customer must pay to the Provider any Charges in respect of Services provided to the Customer before the termination of the Agreement; and

(b) the Provider must refund to the Customer any Charges paid by the Customer to the Provider in respect of Services that were to be provided to the Customer after the termination of the Agreement, without prejudice to the parties' other legal rights.

(c) the Provider will allow the Customer to download their data for the purposes of archiving at no charge to the customer.

**19. Subcontracting**

19.1 The Provider must not subcontract any of its obligations under the Agreement without the prior written consent of the Customer, providing that the Customer must not delay the giving of such consent.

19.2 The Provider shall remain responsible to the Customer for the performance of any subcontracted obligations.

19.3 Notwithstanding the provisions of this Clause 19 but subject to any other provision of these Terms and Conditions, the Customer acknowledges and agrees that the Provider may subcontract to any reputable third party hosting business the hosting of the Platform and the provision of services in relation to the support and maintenance of elements of the Platform.

**20. General**

20.1 No breach of any provision of the Agreement shall be waived except with the express written

consent of the party not in breach.

20.2 If any provision of the Agreement is determined by any court or other competent authority to be unlawful and/or unenforceable, the other provisions of the Agreement will continue in effect. If any unlawful and/or unenforceable provision would be lawful or enforceable if part of it were deleted, that part will be deemed to be deleted, and the rest of the provision will continue in effect (unless that would contradict the clear intention of the parties, in which case the entirety of the relevant provision will be deemed to be deleted).

20.3 The Agreement may not be varied except by a written document signed by or on behalf of each of the parties.

20.4 The Customer hereby agrees that the Provider may assign the Provider's contractual rights and obligations under the Agreement to any successor to all or a substantial part of the business of the Provider from time to time. The Customer must not without the prior written consent of the Provider assign, transfer or otherwise deal with any of the Customer's contractual rights or obligations under the Agreement.

20.5 The Agreement is made for the benefit of the parties, and is not intended to benefit any third party or be enforceable by any third party. The rights of the parties to terminate, rescind, or agree any amendment, waiver, variation or settlement under or relating to the Agreement are not subject to the consent of any third party.

20.6 Subject to Clause 15.1, these Terms and Conditions and any Schedules (including the Services Order Form), shall constitute the entire agreement between the parties, and shall supersede all previous agreements, arrangements and understandings between the parties in respect of that subject matter.

20.7 The Agreement shall be governed by and construed in accordance with English law.

20.8 The courts of England shall have exclusive jurisdiction in respect of any dispute (whether contractual or otherwise) arising under or in connection with the Agreement.

20.9 Nothing in the Agreement is intended to, or shall be deemed to, constitute a partnership or joint venture of any kind between any of the parties, nor constitute any party the agent of another party for any purpose. No party shall have authority to act as agent for, or to bind, the other party in any way.

20.10 The parties acknowledge that the Provider's engagement under this Agreement is as an independent contractor and shall not be deemed employment and/or create a relationship of employment, including without limitation for the purposes of the UK off-payroll working rules including any relevant primary and secondary legislation and the published practice and guidance of HMRC as enacted, amended or made available from time to time. The Provider undertakes to pay all tax, employment claims (including without limitation income tax), National Insurance contributions, statutory sick pay, holiday pay, duties, fees, levies and other impositions (including without limitation in relation to IR35) arising under or in connection with this Agreement and to indemnify the Customer against any cost, claim, expense, liability, penalty, fine or interest in respect of any failure by the Provider to do so.

**21. Interpretation**

21.1 In these Terms and Conditions, a reference to a statute or statutory provision includes a reference to:

(a) that statute or statutory provision as modified, consolidated and/or re-enacted from time to time; and

(b) any subordinate legislation made under that statute or statutory provision.

21.2 The Clause headings do not affect the interpretation of these Terms and Conditions.

21.3 References in these Terms and Conditions to "calendar months" are to the 12 named periods (January, February and so on) into which a year is divided.

21.4 In these Terms and Conditions, general words shall not be given a restrictive interpretation by reason of being preceded or followed by words indicating a particular class of acts, matters or things.

**22. Bribery, corruption, slavery and human trafficking**

22.1 In performing its obligations under this Agreement, the Provider shall:

(a) comply with all applicable anti-slavery, human trafficking and anti-bribery & corruption laws, statutes, regulations from time to time in force including but not limited to the Modern Slavery Act 2015, the Criminal Finances Act 2017 and Bribery Act 2010;

(b) not engage in any activity, practice or conduct that would constitute an offence under sections 1, 2 or 4, of the Modern Slavery Act 2015 and/or sections 1, 2 or 6 of the Bribery Act 2010 if such activity, practice or conduct were carried out in the UK;

(c) include in contracts with its direct subcontractors and suppliers provisions which are at least as onerous as those set out in this Clause 22;

(d) notify the Customer as soon as it becomes aware of any actual or suspected slavery, human trafficking, bribery and/or corruption in a supply chain which has a connection with this Agreement;

(e) maintain a complete set of records to trace the supply chain of all Services provided to the Customer in connection with this Agreement;

(f) permit the Customer and its third party representatives to inspect the Provider's premises, records, and to meet the Provider's personnel to audit the Provider's compliance with its obligations under this Clause 22; and

(g) maintain its own policies and procedures, including but not limited to adequate procedures in connection with the Bribery Act 2010, to ensure the prevention of slavery, human trafficking, bribery and/or corruption within its supply chain.

22.2 The Provider represents and warrants that:

(a) it has not been convicted of any offence involving slavery, human trafficking, bribery, fraud, dishonesty, tax evasion and/or corruption; and

(b) it has not been the subject of any investigation, inquiry or enforcement proceedings regarding any offence or alleged offence of or in connection with slavery, human trafficking, bribery, dishonest conduct, tax evasion and/or corruption.

22.3 The Customer may terminate this Agreement with immediate effect by giving written notice to the Provider if the Provider commits a breach of this Clause 22.

**23. Anti-facilitation of tax evasion**

23.1 The Provider shall:

(a) not engage in any activity, practice or conduct which would constitute either:

- a UK tax evasion facilitation offence under section 45(5) of the Criminal Finances Act 2017; or

- a foreign tax evasion facilitation offence under section 46(6) of the Criminal Finances Act 2017;

(b) comply with the Customer's ethics, anti-bribery and anti-corruption policies (copies of such policies are available on request);

(c) have and shall maintain in place throughout the term of this Agreement such policies and procedures as are both reasonable to prevent the facilitation of tax evasion by another person (including without limitation employees of the Provider) and to ensure compliance with Clause 23.1(a);

(d) notify the Customer in writing if it becomes aware of any breach of Clause 23.1(a) or has reason to believe that it or any person associated with it has received a request or demand from a third party to facilitate the evasion of tax within the meaning of Part 3 of the Criminal Finances Act 2017, in connection with the performance of this Agreement; and

(e) within six months of the date of this Agreement, and annually thereafter, certify to the Customer in writing signed by an officer of the Provider, compliance with this Clause 23.1 by the Provider and all persons associated with it under Clause 23.2. The Provider shall provide such supporting evidence of compliance as the Customer may reasonably request.

23.2 The Provider shall ensure that any person associated with the Provider who is performing Services in connection with this Agreement does so only on the basis of a written contract which imposes on and secures from such person terms equivalent to those imposed on the Provider in this Clause 23 (the "**Relevant Terms**"). The Provider shall be responsible for the observance and performance by such persons of the Relevant Terms, and shall be directly liable to the Customer for any breach by such persons of any of the Relevant Terms.

23.3 Breach of this Clause 23 shall be deemed a material breach under Clause 17.2.

23.4 For the purposes of this Clause 23, the meaning of reasonable prevention procedure shall be determined in accordance with any guidance issued under section 47 of the Criminal Finances Act 2017 and a person associated with the Provider includes but is not limited to any subcontractor of the Provider.

**24. FOIA and EIR**

24.1. The Provider acknowledges that the Customer is subject to the requirements of the FOIA and EIR and shall assist and co-operate with the Customer (at the Provider's expense) to enable the Customer to comply with these information disclosure requirements regarding information relating to the Services.

24.2. The Provider shall and shall procure that its subcontractors shall:

24.2.1. transfer the Request for Information relating to the Services delivered to the Customer as soon as practicable after receipt and in any event within two Business Days of receiving a Request for Information;

24.2.2. provide the Customer with a copy of all Information in its possession or power in the form that the Customer requires within five (5) Business Days (or such other period as the Customer may specify) of the Customer requesting that Information; and

24.2.3. provide all necessary assistance and any representations as to why an exemption to disclosure under the FOIA or an exception to disclosure under the EIR applies as reasonably requested by the Customer to enable the Customer to respond to a Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the EIR.

24.3. The Customer shall be responsible for determining at its absolute discretion whether any Information:

24.3.1. is exempt from disclosure in accordance with the provisions of the FOIA or the EIR; and/or

24.3.2. is to be disclosed in response to a Request for Information

24.4. In no event shall the Provider respond directly to a Request for Information unless expressly authorised to do so by the Customer.

24.5. The Provider acknowledges that the Customer may, acting in accordance with the Secretary of State for Constitutional Affairs' Code of Practice on the discharge of Public Authorities' functions under Part 1 of FOIA (issued under section 45 of the FOIA, November 2004), and the equivalent Code of Practice issued under Regulation 16 of the EIR will be obliged under the FOIA or the EIR to disclose Information:

24.5.1. without consulting with the Provider; or

24.5.2. following consultation with the Provider and having taken its views into account,

provided always that where Clause 24.5.2 applies the Customer shall, in accordance with any recommendations of the Code, take reasonable steps, where appropriate, to give the Provider advanced notice, or failing that, to draw the disclosure to the Provider 's attention after any such disclosure.

24.6. The Provider shall ensure that all information produced in the course of this Agreement or relating to this Agreement is retained for disclosure and shall permit the Customer to inspect such records as requested from time to time.

24.7. The Provider acknowledges that any details provided by it outlining information that it considers to be confidential or commercially sensitive are of indicative value only and that the Customer may nevertheless be obliged to disclose such information in accordance with Clause 24.5.

**Schedule 1 (Acceptable Use Policy)**

**1. Introduction**

1.1 This acceptable use policy (the "**Policy**") sets out the rules governing:

(a) the use of the website at www.secure.propellerpowered.co.uk, any successor website, and the services available on that website or any successor website (the "**Services**"); and

(b) the transmission, storage and processing of content by you, or by any person on your behalf, using the Services ("**Content**").

1.2 References in this Policy to "you" are to any customer for the Services and any individual user of the Services (and "your" should be construed accordingly); and references in this Policy to "us" are to Propeller Powered (and "we" and "our" should be construed accordingly).

1.3 By using the Services, you agree to the rules set out in this Policy.

1.4 We will ask for your express agreement to the terms of this Policy before you upload or submit any Content or otherwise use the Services.

1.5 You must be at least 18 years of age to use the Services; and by using the Services, you warrant and represent to us that you are at least 18 years of age.

**2. General usage rules**

2.1 You must not use the Services in any way that causes, or may cause, damage to the Services or impairment of the availability or accessibility of the Services.

2.2 You must not use the Services:

(a) in any way that is unlawful, illegal, fraudulent or harmful; or

(b) in connection with any unlawful, illegal, fraudulent or harmful purpose or activity.

2.3 You must ensure that all Content complies with the provisions of this Policy.

**3. Unlawful Content**

3.1 Content must not be illegal or unlawful, must not infringe any person's legal rights, and must not be capable of giving rise to legal action against any person (in each case in any jurisdiction and under any applicable law).

3.2 Content, and the use of Content by us in any manner licensed or otherwise authorised by you, must not:

(a) be libellous or maliciously false;

(b) be obscene or indecent;

(c) infringe any copyright, moral right, database right, trade mark right, design right, right in passing off, or other intellectual property right;

(d) infringe any right of confidence, right of privacy or right under data protection legislation;

(e) constitute negligent advice or contain any negligent statement;

(f) be in contempt of any court, or in breach of any court order;

3.3 You must ensure that Content is not and has never been the subject of any threatened or actual legal proceedings or other similar complaint.

**Schedule 2 (Service Level Agreement)**

| Severity Level | What does this severity level mean to the customer? | Response Times |
|---|---|---|
| Severity 1<br>*BusinessCritical* | Impacts all users<br>At least one business critical high impact process inoperable<br>Whole application inoperable<br>Very high commercial impact<br>e.g. system inoperable, Business Application inaccessible | 2 working hours |
| Severity 2<br>*FunctionCritical* | Impacts a majority of users<br>Business Critical but with short term alternatives<br>One section of the application inoperable<br>High commercial impact<br>e.g. The loss of use of applications as shown above, but does not affect everyone. | 4 working hours |
| Severity 3<br>*LimitedImpact* | Impacts on a very limited number of users No critical impact on the business<br>Minor impact on the operability of the application Medium commercial impact<br>e.g. Requires assistance to get: a process working, data backups created, Single non-critical device failure, fixing an error message that has not caused the system to shut down. | 3 working days |
| Severity 4<br>*CosmeticImpact/ How do I?* | Minor cosmetic functionality errors which are not causing an immediate negative impact on the system<br>Minimal impact on users<br>Minimal impact on the operability<br>e.g. General requests for minor amendments or functionality changes that are not causing an immediate negative impact on the system. | 2 weeks |
| Requests for Change / Wish | These are passed on to your Account Manager | No service level |

**Schedule 3 – Software and Services to be provided.**

| PROPELLER SOFTWARE | Qty | Price | Total |
|---|---|---|---|
| (Software details to be entered here) | | | |
| | | | |
| | | | |
| | | | |

| IMPLEMENTATION and ASSOCIATED ADDITIONAL SERVICES | Days | Rate | Total |
|---|---|---|---|
| **(Implementation and Associated Additional Services detail to be added here)** | | | |
| | | | |
| **TOTAL SERVICES (Exc VAT)** | | | |

**Notes to be added here**

| **Signed** | **Propeller Powered Limited** | **(Client Name)** |
|---|---|---|
| **Name** | David Carr | |
| **Title** | Managing Director | |
| **Signature** | | |
| **Date** | | |

**Schedule 4 – Data processing.**

## 1. Data protection

1.1. The Parties acknowledge that for the purposes of Data Protection Legislation, the Council is the Controller and the Consultant is the Processor. The only processing that the Processor is authorised to do is listed in Annex A by the Controller and may not be determined by the Processor. The term "processing" and any associated terms are to be read in accordance with the Data Protection Legislation.

1.2. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe Data Protection Legislation.

1.3. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:

1.3.1. a systematic description of the envisaged processing operations and the purpose of the processing;

1.3.2. an assessment of the necessity and proportionality of the processing operations in relation to the Services;

1.3.3. an assessment of the risks to the rights and freedoms of Data Subjects; and

1.3.4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4. The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

1.4.1. process that Personal Data only in accordance with Annex A unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

1.4.2. ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject. In the event of the Controller reasonably rejecting Protective Measures put in place by the Processor, the Processor must propose alternative Protective Measures to the satisfaction of the Controller. Failure to reject shall not amount to approval

by the Controller of the adequacy of the Protective Measures. Protective Measures must take account of the:

1.4.2.1. nature of the data to be protected;

1.4.2.2. harm that might result from a Data Loss Event;

1.4.2.3. state of technological development; and

1.4.2.4. cost of implementing any measures;

1.4.3. ensure that:

1.4.3.1. the Consultant Personnel do not process Personal Data except in accordance with this Agreement (and in particular this Schedule);

1.4.3.2. it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

1.4.3.2.1. are aware of and comply with the Processor's duties under this paragraph;

1.4.3.2.2. are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

1.4.3.2.3. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and

1.4.3.2.4. have undergone adequate training in the use, care, protection and handling of Personal Data; and

1.4.3.2.5. not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(i) the destination country has been recognised as adequate by the UK government in accordance with Article 45 UK GDPR or section 74 of the DPA 2018;

(ii) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 DPA 2018) as determined by the Controller;

(iii) the Data Subject has enforceable rights and effective legal remedies;

(vi) the Processor complies with its obligations under Data Protection Legislation by providing an appropriate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

(v) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

(vi) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Agreement unless the Processor is required by Law to retain the Personal Data.

1.5. Subject to paragraph 1.6, the Processor shall notify the Controller immediately if it:

1.5.1. receives a Data Subject Request (or purported Data Subject Request);

1.5.2. receives a request to rectify, block or erase any Personal Data;

1.5.3. receives any other request, complaint or communication relating to either Party's obligations under Data Protection Legislation;

1.5.4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

1.5.5. receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

1.5.6. becomes aware of a Data Loss Event.

1.6. The Processor's obligation to notify under paragraph 1.5 shall include the provision of further information to the Controller, as details become available.

1.7. Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 1.5 (and insofar as possible within the timescales reasonably required by the Controller) including but not limited to promptly providing:

1.7.1. the Controller with full details and copies of the complaint, communication or request;

1.7.2. such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in Data Protection Legislation;

1.7.3. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

1.7.4. assistance as requested by the Controller following any Data Loss Event;

1.7.5. assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

1.8. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this paragraph. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

1.8.1. the Controller determines that the processing is not occasional;

1.8.2. the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

1.8.3. the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

1.10. Each Party shall designate its own data protection officer if required by Data Protection Legislation.

1.11. Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:

1.11.1. notify the Controller in writing of the intended Sub-processor and processing;

1.11.2. obtain the written consent of the Controller;

1.11.3. enter into a written agreement with the Sub-processor which give effect to the terms set out in this schedule such that they apply to the Sub-processor; and

1.11.4. provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

1.12. The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

1.13. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may upon giving the Processor not less than 30 working days' notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

## Annex A

## Processing, Personal Data and Data Subjects

This Schedule shall be completed by the Controller, who may take account of the view of the
Processor, however the final decision as to the content of this Schedule shall be with the Controller at its absolute discretion.

1. The contact details of the Controller's Data Protection Officer are: [Insert Contact details]
2. The contact details of the Processor's Data Protection Officer are: Steve Senior steve.senior@teampropeller.co.uk
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
4. Any such further instructions shall be incorporated into this Schedule.

| **Description** | **Details** |
|---|---|
| Subject matter of the processing | The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide the Services. |
| Duration of the processing | The duration of this Agreement |
| Nature and purposes of the processing | The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. |

| Description | Details |
|---|---|
| | The purpose includes for the provision of the Services. |
| Type of Personal Data being Processed | name, address, telephone number, email. |
| Categories of Data Subject | Staff (including volunteers, agents, and temporary workers), clients, consultants, members of the public. |
| International transfers and legal gateway | All personal data must remain within the UK and may only be transferred outside the UK with the written consent of the Controller |
| Plan for return and destruction of the data once the processing is complete | All data should be returned to the council at the expiry or termination of the Agreement and any Order and securely destroyed. |

## Annex B: Security

The technical security requirements set out below provide an indication of the types of security measures that might be considered, in order to protect Personal Data.

More, or less, measures may be appropriate depending on the subject matter of the contract, but the overall approach must be proportionate. The technical requirements must also be compliant with legislative and regulatory obligations for content and data, such as UK GDPR.

The example technical security requirements set out here are intended to supplement, not replace, security schedules that will detail the total contractual security obligations and requirements that the Processor (i.e. a Consultant) will be held to account to deliver under contract.

Processors are also required to ensure sufficient 'flow-down' of legislative and regulatory obligations to any third party Sub-processors.

**External Certifications** e.g. Buyers should ensure that Consultants hold at least Cyber Essentials Plus certification and ISO 27001:2013 certification if proportionate to the service being procured.

**Risk Assessment** e.g. Consultant should perform a technical information risk assessment on the service supplied and be able to demonstrate what controls are in place to address those risks.

**Security Classification of Information** e.g. If the provision of the Services requires the Consultant to Process Council/Buyer Data which is classified as OFFICIAL,OFFICIAL-SENSITIVE or Personal Data, the Consultant shall implement such additional measures as agreed with the Council/Buyer from time to time in order to ensure that such information is safeguarded in accordance with the applicable legislative and regulatory obligations.

**End User Devices** e.g.

- The Consultant shall ensure that any Council/Buyer Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Council/Buyer except where the Council/Buyer has given its prior written consent to an alternative arrangement.

- The Consultant shall ensure that any device which is used to Process Council/Buyer Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security.

**Testing** e.g. The Consultant shall at their own cost and expense, procure a CHECK or CREST Certified Consultant to perform an ITHC or Penetration Test prior to any live Council/Buyer data being transferred into their systems. The ITHC scope must be agreed with the Council/Buyer to ensure it covers all the relevant parts of the system that processes, stores or hosts Council/Buyer data.

**Networking** e.g. The Consultant shall ensure that any Council/Buyer Data which it causes

to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

**Personnel Security** e.g. All Consultant Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard or equivalent including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record. The Consultant maybe required to implement additional security vetting for some roles.

**Identity, Authentication and Access Control** e.g. The Consultant must operate an appropriate access control regime to ensure that users and administrators of the service are uniquely identified. The Consultant must retain records of access to the physical sites and to the service.

**Data Destruction/Deletion** e.g. The Consultant must be able to demonstrate they can supply a copy of all data on request or at termination of the service, and must be able to securely erase or destroy all data and media that the Council/Buyer data has been stored and processed on.

**Audit and Protective Monitoring** e.g. The Consultant shall collect audit records which relate to security events in delivery of the service or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Consultant audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the service, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Council/Buyer Data. The retention periods for audit records and event logs must be agreed with the Council/Buyer and documented.

**Location of Council/Buyer Data** e.g. The Consultant shall not, and shall procure that none of its Sub-contractors, process Council/Buyer Data outside the EEA without the prior written consent of the Council/Buyer and the Consultant shall not change where it or any

of its Sub-contractors process Council/Buyer Data without the Council/Buyer's prior written consent which may be subject to conditions.

**Vulnerabilities and Corrective Action** e.g. Consultants shall procure and implement security patches to vulnerabilities in accordance with the timescales specified in the NCSC Cloud Security Principle 5.

Consultants must ensure that all COTS Software and Third Party COTS Software be kept up to date such that all Consultant COTS Software and Third Party COTS Software are always in mainstream support.

**Secure Architecture** e.g. Consultants should design the service in accordance with:

- NCSC "Security Design Principles for Digital Services"
- NCSC "Bulk Data Principles"
- NSCS "Cloud Security Principles"