

ORDER FORM



online service network

Date 27/03/20 No. R2CJC00168MAR Cust. P.O. No. Minimum Term (months) 24

Company Details

Company (Full name/s of company, sole trader, partners):
 Highways England Company Ltd
 Trading as: Highways England
 Contact Name: Jo Pavely
 Position: Procurement Partner
 Website: https://highwaysengland.co.uk/
 Parent Company: N/A
 Industry: Public Sector

Address: Bridge House
 1 Walnut Tree Close
 Town/City: Guildford
 Post Code: GU1 4LZ
 Telephone: 0300 470 8306 Fax:
 Email: Jo.Pavely@highwaysengland.co.uk
 Accounts Email:
 Type of Customer: Operator
 Company Registration No.: 09346363

Quantity	Unit Type	Product Description	*Monthly Unit Cost	Total Monthly Payments
1000	Assets	r2c Operator Core	█	█
1000	Assets	r2c Vantage Point	█	█
1000	Assets	r2c issue2invoice	█	█

First Payment █
 Followed by 21
 Payments of █
 Payment Frequency Monthly

The First Payment will be due on signature of this agreement or on any date after that we decide, First quarter deposit then monthly in advance by automated payment (Direct Debit) commencing in the second month, collected within a minimum of 10 days of the Invoice Date. All implementation and training costs are added to the first payment. All Monthly Payments and Other Charges exclude VAT to be added at the prevailing rate.

Sub Total █
 VAT █
 TOTAL £4680

OTHER CHARGES PAYABLE ON DELIVERY

Quantity	Product Description	Unit Price	Total
3	Implementation & Set up (Including imports)	█	█
3	Project Management	█	█
2	Onsite / Online Training	█	█
	Additional Services charged at █ per day		

Sub Total █
 VAT █
 TOTAL £7680

Please note the above costs are budget only. Travel and expenses costs will be charged separately as incurred. Cancellation or amendments to training dates can be made without charge at any time 10 days prior to the original booked date. If changes to dates or cancellations are made within 10 days then 50% of the training costs will be payable and within 5 working days 100% of the costs will be payable.

Special Notes

This order represents a minimum contract value. Any additional users, assets or transactions above the minimum will be chargeable at the end of each month at the unit rate quoted.

Implementation Instructions

Contact: Jo Pavely
 Position:
 Implementation Address
 Town/City:
 County:
 Post Code:

Email:
 Telephone:
 Fax:
 Asset Type:
 No. of Assets:
 Implementation Date:
 Implementation Contact:

We agree to comply with and be bound by the terms of trade printed overleaf.

Customer Name (PRINT):
 Position: Date:
 Customer Signature:

Representative Name (PRINT):
 Date:
 Representative Signature:



Highways England Company Limited

NEC3 Term Service Short Contract
(April 2013)

Form of Agreement

in relation to *services* for

Fleet Management Software

THIS AGREEMENT is made the Third day of April 2020.

PARTIES:

1. **HIGHWAYS ENGLAND COMPANY LIMITED** (company number 09346363) whose registered address is at Bridge House, 1 Walnut Tree Close, Guildford, Surrey GU1 4LZ ("the *Client*"); and
2. **R2C ONLINE LIMITED (company number 04978908)** whose registered address is at 2 Vantage Drive, Sheffield, S9 1RG ("the *Contractor*").

RECITALS

- (A) In response to the Client's invitation to tender, the Contractor has submitted a tender to carry out and complete the following service : the provision of the Fleet Management Software accordance with the Service Information.
- (B) The Client has accepted the Contractor's tender by letter dated 18th March and now wishes to appoint the Contractor on the terms of this Agreement.

IT IS AGREED

OPERATIVE PROVISIONS

1. Definitions and Interpretation

- 1.1 In this Agreement (including the Recitals) words and expressions have the same meaning given to them in the Conditions referred to below.
- 1.2. The Conditions are the core clauses of the NEC3 Term Service Short Contract and any additional Z clauses.
- 1.3 The Contractor's terms are the standard terms and conditions and service level agreement as amended from time to time as provided to the Client.

2. Documents

- 3.1 The documents forming part of this Agreement are:
 1. the Conditions (Highways England & r2c Online Ltd Terms and Conditions)
 2. the Contract Data
 3. the Service Information
 4. r2c Online core platform and Vantage Point specifications from time to time
 5. r2c Online Standard Terms and Conditions as amended from time to time
 6. r2c Online Service Level Agreement as amended from time to time
 7. r2c Online Ltd The Price List (18 March 2020)
- 3.2. The several documents forming part of this Agreement are to be taken as mutually explanatory of one another.
- 3.3 If there is any conflict or ambiguity between the terms of the documents listed in clause 3.1 or if the Conditions or the Contract Data is silent then the following shall apply:

- 3.3.1 if there is any conflict or ambiguity regarding termination then the Contractor's Standard Terms shall prevail;
- 3.3.2. if there is any conflict or ambiguity regarding confidentiality then the Contractor's Standard Terms shall prevail;
- 3.3.3 if there is any conflict or ambiguity regarding force majeure then the Conditions shall prevail;
- 3.3.4 if there is any conflict or ambiguity regarding liability then the Conditions shall prevail save for where the Conditions are silent then the Contractor's Standard Terms shall prevail.
- 3.3.5 if the Conditions or Contract Data is silent on terms regarding provision of the Contractor's online platform then the Contractor's Standard Terms and/or core platform and Vintage Point specifications shall prevail;
- 3.3.6 if there is any conflict or ambiguity regarding Intellectual Property Rights the Contractor's Standard Terms shall prevail.

Signed by Jo Paveley

for and on behalf of **HIGHWAYS ENGLAND COMPANY LIMITED**

.....

Authorised Signatory

Signed by Joe Clarke

for and on behalf of **R2C ONLINE LIMITED**

.....

Authorised Signatory

Highways England

Term Service Short Contract

Contract Data and *Contractor's Offer*

Contract Data

Part one – Data provided by the *Employer*

The Data which will apply to all work under the Contract is

- The *conditions of this contract* are the clauses of the NEC3 Term Service Short Contract (April 2013) and the additional clauses in Appendix A.
- The *Employer* is Highways England Company Limited, a company incorporated in and in accordance with the laws of England and Wales, having as its registered number 09346363 of Bridge House, 1 Walnut Tree Close, Guildford, Surrey, GU1 4LZ.
- Contact details for Project manager are:
Martin Edgecox, Martin.Edgecox@highwaysengland.co.uk, 07702 972 842,
The Cube, 199 Wharfside Street, Birmingham, B1 1RN.
- The *service* is Fleet Management Software.
- The Service Information is in the document entitled “Service Information”.
- The *starting date* is the award date.
- The *service period* is: 24 months
- The *period for reply* is 5 working days.
- The assessment day is the seventh working day of each month
- Does the Housing Grants Construction and Regeneration Act 1996 (as amended by the Local Democracy, Economic Development and Construction Act 2009 apply? No
- The *Adjudicator* is the person chosen by the Parties from the list of Adjudicators published by the Chartered Institute of Arbitrators.
- The *law of the contract* is the law of England and Wales, subject to the jurisdiction of the Courts of England and Wales.
- The interest rate on late payment is, unless the provisions of the Late Payment of Commercial Debts (Interest) Act 1998 otherwise require, 3% per annum above the Bank of England base rate in force from time to time.

The minimum amount of cover for the first insurance stated in the Insurance Table is a limit of indemnity of not less than one million pounds (£1,000,000) in respect of any one occurrence, the number of occurrences being unlimited in any annual policy period.
- The minimum amount of cover for the third insurance stated in the Insurance Table is a limit of indemnity of not less than one million pounds

(£1,000,000) in respect of any one occurrence, the number of occurrences being unlimited in any annual policy period.

- The minimum amount of cover for the fourth insurance stated in the Insurance Table is a limit of indemnity of one million pounds (£1,000,000) any one occurrence the number of occurrences being unlimited in any annual policy period or as required by statute whichever is the higher
- The *Contractor* is not liable to the *Employer* for loss of or damage to the *Employers* property in excess of five hundred thousand pounds (£500,000).
- The *Adjudicator nominating body* is Chartered Institute of Arbitrators
- The *tribunal* is arbitration.
- If the *tribunal* is arbitration the arbitration procedure is the Chartered Institute of Arbitrators' Arbitration Rules (2000)
- The *currency of this contract* is the pound sterling (£).

Contract Data

Part 2 The *Contractor's Offer*

The Data which will apply to all work under the contract is

- The *Contractor* is
 - Name
 - Address
 - Telephone
 - E-mail address
- The Quality Statement is in.....
- The Software Schedule is Not Used.
- The percentage for overheads and profit added to Defined Cost for people is%
- The percentage for overheads and profit added to other Defined Cost is%
- The offered total of the Prices for the *service* is

Appendix A

- Option Z** • **The additional conditions of contract are clauses Z1 - Z27**

Clause Z1 Corrupt practices

Z1.1 The *Contractor* does not

- offer or give to any person in the service of the *Employer* any gift or consideration of any kind as an inducement or reward in relation to the obtaining or execution of this contract or any other contract with the *Employer* or for showing favour or disfavour to any person in relation to this contract or any other contract with the *Employer* or
- enter into this contract or any other contract with the *Employer* if, in connection with this contract or any such other contract, commission has been paid or an agreement for the payment of commission has been made by him or on his behalf or to his knowledge.

Z1.2 A failure to comply with this condition is treated as a substantial failure by the *Contractor* to comply with this contract.

Clause Z2 Recovery of sums due from *Contractor*

Z2.1 Where under this contract any sum of money is recoverable from or payable by the *Contractor*, such sum may be deducted from or reduced by the amount of any sum or sums then due or which at any time after may become due to the *Contractor* under this contract or any other contract with any Department or Office of Her Majesty's Government.

Clause Z3 Assignment

Z3.1 The *Contractor* does not assign, transfer or charge the benefit of this contract or any part of it or any benefit or interest under it without the prior agreement of the *Employer*.

Z3.2 The *Employer's* ability to assign this contract or any part of it or any benefit or interest under it is unrestricted.

Z3.3 If requested by the *Employer*, the *Contractor* executes an agreement in the form set out in the Service Information (Appendix D) or such other form as the *Employer* may reasonably require to novate the benefit and burden of the contract or any Task Order to

- a Department or Office of Her Majesty's Government,
- a local authority,
- a replacement organisation established to take over the *Employer's* functions or part of them or

- another public body exercising similar functions.

Clause Z4 Disclosure of information

- Z4.1 A Disclosure Request is a request for information relating to this contract received by *Employer* pursuant to the Freedom of Information Act 2000, the Environmental Information Regulation 2004 or otherwise.
- Z4.2 The *Contractor* acknowledges that the *Employer* may receive Disclosure Requests and that the *Employer* may be obliged (subject to the application of any relevant exemption and, where applicable, the public interest test) to disclose information (including commercially sensitive information) pursuant to a Disclosure Request. Where practicable, the *Employer* consults with the *Contractor* before doing so in accordance with the relevant Code of Practice. The *Contractor* uses its best endeavours to respond to any such consultation promptly and within any deadline set by the *Employer* and acknowledges that it is for the *Employer* to determine whether or not such information should be disclosed.
- Z4.3 When requested to do so by the *Employer*, the *Contractor* promptly provides information in its possession relating to this contract and assists and co-operates with the *Employer* to enable the *Employer* to respond to a Disclosure Request within the time limit set out in the relevant legislation.
- Z4.4 The *Contractor* promptly passes any Disclosure Request which it receives to the *Employer*. The *Contractor* does not respond directly to a Disclosure Request unless instructed to do so by the *Employer*.
- Z4.5 A Disclosure Request is a request for information relating to this contract received by the *Employer* pursuant to the Freedom of Information Act 2000, the Environmental Information Regulations 2004 or otherwise.
- Z4.6 The *Contractor* acknowledges that the *Employer* is obliged to publish the provisions of this contract in accordance with the Cabinet Office Efficiency Reform Group Procurement Policy Note entitled "*Published guidance on implementing requirements for greater transparency in central Government procurement and contracting*" (Information Note 02/11 dated 18 January 2011, or any later revision), except to the extent that any information in it is exempt from disclosure pursuant to the Freedom of Information Act 2000. The *Employer* consults with the *Contractor* before deciding whether information is exempt, but the *Contractor* acknowledges that the *Employer* has the final decision. The *Contractor* co-operates with and assists the *Employer* to publish this contract in accordance with the *Employer's* obligation.

Clause Z5 Official Secrets Act

- Z5.1 The Official Secrets Acts 1989 apply to this contract from the *starting date* until the *defects date* or earlier termination.
- Z5.2 The *Contractor* notifies his employees and his subcontractors of their duties under this act.
- Z5.3 A failure to comply with this condition is treated as a substantial failure by the *Contractor* to comply with this contract.

Clause Z6 Staff Vetting and Training

- Z6.1 The *Contractor* complies with the staff vetting and training requirements stated in the Service Information.

Clause Z7 Confidentiality

- Z7.1 The *Contractor* keeps (and ensures that anyone employed by it or acting on its behalf keeps) confidential and does not disclose to any person the terms of this contract or
- use (except for the purposes of this contract) or disclose to any person, any confidential or proprietary information (including Personal Data) provided to or acquired by the *Contractor* in the course of Providing the Service
- except that the *Contractor* may disclose information
- to its legal or professional advisers
 - to its employees and subcontractors as needed to enable the *Contractor* to Provide the Service,
 - where required to do so by law or by any professional or regulatory obligation or by order of any court or government agency, provided that prior to disclosure the *Contractor* consults the *Employer* and takes full account of the *Employer's* views about whether (and if so to what extent) the information should be disclosed
 - which it receives from a third party who lawfully acquired it and who is under no obligation restricting its disclosure,
 - which is in the public domain at the time of disclosure other than due to the fault of the *Contractor* or
 - with the consent of the *Employer*.

Clause Z8 Conflict of interest

- Z8.1 In accordance with section 3 of the Service Information, if the *Contractor* or subcontractor (at any stage of remoteness from the *Employer*) notifies the *Employer* of a conflict of interest, the *Employer* may require the *Contractor* to stop Providing the Service until any conflict of interest is resolved.
- Z8.2 Any steps taken in accordance with clause Z8.1 above, section 3 in the Service Information, or an instruction from the *Employer* to the *Contractor* to restart work once the conflict of interest is resolved is not a compensation event.
- Z8.3 A failure to comply with section 3 in the Service Information is treated as the *Contractor* having substantially hindered the *Employer* or Others.

Clause Z9 Subcontracting- PCRs Regulation 57 and 59.

- Z9.1 Before
- appointing a proposed subcontractor or
 - allowing a subcontractor to appoint a proposed subsubcontractor
- the *Contractor* submits to the *Employer* for acceptance
- a European Single Procurement Document (as described in regulation 59 of the Public Contracts Regulations 2015, as amended) in respect of the proposed subcontractor or sub-subcontractor or
 - other means of proof that none of the mandatory or discretionary grounds for exclusion referred to in regulation 57 of the Public Contracts Regulations 2015, as amended applies to the proposed subcontractor or sub-subcontractor.
- Z9.2 The *Contractor* does not appoint the proposed subcontractor (or allow the subcontractor to appoint the proposed sub-subcontractor) until the *Employer* has accepted the submission. A reason for not accepting the submission is that it shows that there are grounds for excluding the proposed subcontractor or sub-subcontractor under regulation 57 of the Public Contracts Regulations 2015, as amended.
- Z9.3 If requested by the *Employer*, the *Contractor* provides further information to support, update or clarify a submission under clause Z9.1.
- Z9.4 If, following the acceptance of a submission under clause Z9.2, it is found that one of the grounds for excluding the subcontractor or sub-subcontractor under regulation 57 of the Public Contracts Regulations 2015, as amended applies, the *Employer* may instruct the *Contractor* to

- replace the subcontractor or
- require the subcontractor to replace the sub-subcontractor.

Clause Z10 Records and Audit Access

- Z10.1 The *Contractor* keeps documents and information obtained or prepared by the *Contractor* or any subcontractor in connection with this contract for a period of 6 years after the *service period*.
- Z10.2 The *Contractor* permits the *Employer* and/or anyone so authorised by the *Employer* and/or the Comptroller and Auditor General to examine documents held or controlled by the *Contractor* or any subcontractor.
- Z10.3 The *Contractor* provides such oral or written explanations as the *Employer* or the Comptroller and Auditor General considers necessary.
- Z10.4 The *Contractor* acknowledges that, for the purpose of examining and certifying the *Employer's* accounts or any examination pursuant to Section 6(1) of the National Audit Act 1983, the Comptroller and Auditor General or any other auditor appointed by the *Employer* may examine documents held or controlled by the *Contractor* or any subcontractor and may require the *Contractor* to provide such oral or written explanations as he considers necessary. The *Contractor* promptly complies with any such requirements at his own cost. This clause does not constitute a requirement or agreement for the purposes of section 6(3)(d) of the National Audit Act 1983 for the examination, certification or inspection of the accounts of the *Contractor* and the carrying out of an examination under Section 6(3)(d) of the National Audit Act 1983 in relation to the *Contractor* is not a function exercisable under this contract. The *Contractor* permits the Comptroller and Auditor General to examine documents held or controlled by the *Contractor* or any subcontractor. The *Contractor* provides such oral or written explanations as the Comptroller and Auditor General considers necessary.

Clause Z11 Extension of the service period

- Z11.1 The Employer may at any time in its discretion, extend the service period, provided always that the total period of extension does not exceed the extension period.

Clause Z12 Appointment of Adjudicator

- Z12.1 The *Adjudicator's* appointment under the NEC3 Adjudicator's Contract (April 2013) and includes the following additional condition of contract:
- 'The *Adjudicator* complies, and takes all reasonable steps to ensure that any persons advising or aiding him comply, with the Official Secrets Act 1989. Any information concerning the Contract obtained either by the Adjudicator or any person advising or aiding him is

confidential, and may not be used or disclosure by the Adjudicator or any person except for the purpose of this Agreement”.

Clause Z13 Third Party Rights

Z13.1 A subcontractor has the right to enforce the terms of clause Z9.4 (Subcontracting) and Z24 (Fair payment - second bullet) and a Named Supplier has the right to enforce clause Z17 (PBA) if a Project Bank Account is included in the contract. Otherwise a person or organisation who is not a Party has no right to enforce any term of this contract under the Contracts (Rights of Third Parties) Act 1999.

Clause Z14 Publicity

Z14.1 The *Contractor* may publicise this contract only with the *Employer's* written agreement.

Clause Z15 Parent Company Guarantee and Change of Control

Z15.1 In this contract

- **Consortium Member** is an organisation or person which is a member of a group of economic operators comprising the *Contractor*, whether as a participant in an unincorporated joint venture or a shareholder in a joint venture company.
- **Change of Control** is an event where a single person (or group of persons acting in concert)
 - acquires Control of the *Contractor* or a Consortium Member or
 - acquires a direct or indirect interest in the relevant share capital of the *Contractor* or a Consortium Member and as a result holds or controls the largest direct or indirect interest in (and in any event more than 25% of) the relevant share capital of the *Contractor* or a Consortium Member.
- **Control** has the meaning set out in section 1124 of the Corporation Tax Act 2010.
- **Controller** is the single person (or group of persons acting in concert) that
 - has Control of the *Contractor* or Consortium Member or
 - holds or controls the largest direct or indirect interest in the relevant share capital of the *Contractor* or a Consortium Member.
- **Parent Company Guarantee** is a guarantee of the *Contractor's* performance in the form set out in the Service Information.

Z15.2 If required by the *Employer* at any time, the *Contractor* within four weeks gives to the *Employer* a Parent Company Guarantee from

- the Controller or
- if the *Employer* (in its discretion) agrees, a company other than the Controller.

Z15.3 The *Contractor* notifies the *Employer* immediately if a Change of Control has occurred or is expected to occur.

Z15.4 The *Employer* may treat any of the following as a substantial failure by the *Contractor* to comply with this contract

- the *Contractor* does not give to the *Employer* a Parent Company Guarantee within four weeks of the *Employer's* request,
- the *Contractor* fails to notify the *Employer* of a Change of Control or
- a Change of Control will not allow the *Contractor* to perform its obligations under this contract

Z15.5 If the Controller, or any alternative guarantor proposed by the *Contractor*, is not a company incorporated in and subject to the laws of England and Wales or Scotland, the *Contractor* provides a legal opinion from a lawyer or law firm which is

- qualified and registered to practise in the jurisdiction in which the Controller or guarantor is incorporated and
- accepted by the *Employer*.

The legal opinion is addressed to the *Employer* on a full reliance basis and the liability of the lawyer or law firm giving the opinion is not subject to any financial limitation unless otherwise agreed by the *Employer*.

The legal opinion confirms that the method of execution of the Parent Company Guarantee is valid and binding under applicable local law and in particular covers the matters listed in the Service Information.

Clause Z16 *Employer's Codes of Conduct: (Employer's Anti Bribery Code of Conduct and Anti-Fraud Code of Conduct)*

Z16.1 The *Contractor* complies with the *Employer's* Anti Bribery Code of Conduct and Anti-Fraud Code of Conduct, collectively "the Codes". The *Contractor* complies with the Codes until the later of the end of the *service period* and the latest date for the correction of defects after delivery and with

- paragraph 4 of the *Employer's* Anti Bribery Code of Conduct
- paragraph 3 of the *Employer's* Anti-Fraud Code of Conduct.

- for a period of 6 years after the later of the end of the *service period* and the latest date for the correction of defects after delivery.

Z16.2 A failure to comply with this condition is treated as the *Contractor* having substantially failed to comply with this contract.

Z16.3 The *Contractor*

- includes in the conditions of contract for each subcontractor (at any stage of remoteness from the *Employer*) obligations similar to those set out above and
- requires each subcontractor to include obligations similar to those set out above in each sub-subcontract with the intention that all subcontractors (at any stage of remoteness from the *Employer*) include obligations similar to those set out above.

Clause Z17 Not Used

Clause Z18 Not Used

Clause Z19 Termination - PCRs, Regulation 73

Z19.1 The *Employer* may terminate the *Contractor's* obligation to Provide the Service if one of the mandatory or discretionary grounds for exclusion referred to in regulation 57 of the Public Contracts Regulations 2015 applied to the *Contractor* at the *starting date*. The amount due on termination is the same as for Reason 2.

Z19.2 The *Employer* may terminate the *Contractor's* obligation to Provide the Service if

- this contract has been subject to a substantial modification which would have required a new procurement procedure pursuant to regulation 72 of the Public Contracts Regulations 2015 or
- the Court of Justice of the European Union declares, in a procedure under Article 258 of the Treaty on the Functioning of the European Union, that a serious infringement of the obligations under the European Union Treaties and the Public Contracts Directive has occurred.

The amount due on termination is the same as for

- if the modification or infringement was due to a default by the *Contractor* or
- if the modification or infringement was due to any other reason.

Clause Z20 Value Added Tax (VAT) Recovery

Z20.1 Where under this contract any amount is calculated by reference to any sum which has been or may be incurred by any person, the amount shall include any VAT in respect of that amount only to the extent that such VAT is not recoverable as input tax by that person (or a member of the same VAT group) whether by set off or repayment.

Clause Z21 Payment

Z21.1 In clause 50.2 at the end of the second bullet point insert the words “subject to any applicable deduction to the relevant rate in accordance with the Price List or Task Order”.

Clause Z22 Payments upon Insolvency

Z22.1 Nothing in this contract requires the *Employer* to pay the *Contractor* any sum due where the *Contractor* becomes insolvent after the last date upon which the *Employer* was entitled to issue a pay less notice in respect of the relevant sum.

Clause Z23 Changes to rates and prices

Z23.1 The Parties may at any time agree to a reduction to the rates or Prices in the Price List.

Z23.2 The reduced rates or Prices apply to any part of the *service* provided after the reduction is agreed.

Z23.3 If the *Contractor* does not agree a reduction requested by the *Employer*, the *Employer* may terminate the *Contractor's* obligation to Provide the *Service* by notifying the *Contractor*.

Clause Z24 Fair Payment

Z24.1 The *Contractor* assesses the amount due to a subcontractor without taking into account the amount assessed under this contract.

Z24.2 The *Contractor* includes in the contract with each subcontractor

- a provision requiring the *Contractor* to pay the subcontractor within a specified period (not exceeding 19 days after the date on which payment becomes due under this contract) for work which the subcontractor has completed from the previous assessment date up to the current assessment date in this contract,
- a provision requiring the subcontractor to include in each subsubcontract the same requirement, except that the period for payment is not to exceed 23 days after the date on which payment becomes due under this contract,

- a provision requiring the subcontractor to assess the amount due to a subsubcontractor without taking into account the amount paid by the *Contractor* and
- a provision requiring each further stage subcontract to contain provisions to the same effect as these requirements, with the intention that all subcontractors (at any stage of remoteness from the *Employer*) are to be paid within three weeks after the date on which payment becomes due under this contract.

Z24.3 The *Contractor* notifies non-compliance with the timescales for payment

- to the *Employer* and
- through the Efficiency and Reform Group Supplier Feedback Service.

The *Contractor* includes this provision in each subcontract, and requires subcontractors to include the same provision in each subsubcontract with the intention that all subcontractors (at any stage of remoteness from the *Employer*) include the same provision.

Z24.4 A failure to comply with this condition is treated as a *Contractor* having substantially failed to comply with this contract.

Clause Z25 Intellectual Property Rights

Z25.1 **Intellectual Property Rights** or **IPRs** are copyright and related rights, database rights, design rights, patents, inventions, trade marks (and goodwill attaching to those trade marks), domain names, applications for and the right to apply for any of the foregoing, moral rights, confidential information and any other intellectual or industrial property rights, whether or not registered or capable of registration, whether subsisting now or in future in any part of the world.

Z25.2 All Intellectual Property Rights in documents and other materials created by or on behalf of the *Employer* in connection with the contract are the property of the *Employer* or the Crown.

Z25.3 The *Contractor* hereby assigns to the *Employer* all present and future Intellectual Property Rights in all documents and other materials created by or on behalf of the *Contractor* or any subcontractor in performing its obligations under, or otherwise in connection with, the contract. The *Contractor* obtains from subcontractors equivalent rights over the documents and other materials prepared by the subcontractors. This assignment takes effect either on the *starting date* or as a present assignment of future rights that will take effect immediately on the coming into existence of the relevant Intellectual Property Rights, as appropriate.

Z25.4 Contractor's Background IPR means IPR owned by the *Contractor* or a third party before the *starting date* or created by the *Contractor* or a third party independently of this contract, which in each case is or will be used before the end of the *service period* for designing, testing, implementing, correcting Defects or Providing the Service. In respect of the Contractor's Background IPR, the *Contractor* grants a non-exclusive, world-wide, perpetual, irrevocable, royalty free licence (including the right to sub-licence) to the *Employer* to use the Background IPR for all purposes of the *Employer*. Each licence granted under this clause Z24.4 by the *Contractor* survives the termination or expiry of this contract and cannot be terminated by the *Contractor* or its assignees. The *Contractor* obtains from the subcontractors or third parties equivalent rights over the Contractor's Background IPR owned by the subcontractors or third parties.

Z25.5 The *Employer* grants to the *Contractor*, or procures the direct grant to the *Contractor* of, a non-exclusive, non-transferable, revocable licence to use all Intellectual Property Rights and Background IPR owned (or capable of being so licensed or procured without cost) by the *Employer* and reasonably required by the *Contractor* in order to Provide the Service. Any such licence is granted for the duration of this contract solely to enable the *Contractor* to comply with its obligations under this contract.

Clause Z26 Contractor's premises and Access and Storage to Employer's Data

Z26.1 In this clause

Risk Assessment is a full risk assessment and security review carried out by the *Employer* in accordance with this contract.

Offshore is a location outside United Kingdom of Great Britain and Northern Ireland.

Z26.2 Any failure of the *Employer* to gain approval for storing information Offshore or allowing access to information from an Offshore location in accordance with this contract

- is not a compensation event and
- does not relieve the *Contractor* from his obligation to Provide the Service

Z26.3 A failure for a premise to pass the Risk Assessment

- is not a compensation event and
- does not relieve the *Contractor* from his obligation to Provide the Service

Z26.4 The *Contractor* pays for the *Employer's* costs associated with undertaking any Risk Assessment.

Clause Z27 Not Used

Schedule A: r2c Online Ltd Terms and Conditions:

R2C Online: Terms & Conditions

The following terms and conditions set out the basis on which R2C Online Limited (R2C), company number 04978908, registered office R2C Online Ltd, 2 Vantage Drive, Sheffield, South Yorkshire S9 1RG, makes available to you (the Customer) access to application software and data using your internet connection to our remote computer systems.

The Customer agrees to access the Software and Additional Services under these Terms and Conditions.

1. INTERPRETATION

1.1 The following definitions and rules of interpretation apply:

Additional Charges: the charges to be calculated by R2C on a time and materials basis at rates to be

expressly notified in writing to the Customer from time to time in respect of the provision of Additional Services;

Additional Services: any additional services which are not included in the provision of the Software;

Agreement: means R2C's Terms and Conditions set forth herein, the Order Form and R2C's Service Level Agreement (where appropriate);

Authorised Users: those employees and independent contractors of the Customer who are entitled to use the Software and Services under the Agreement;

Business Day: a day (other than a Saturday, Sunday or public holiday) when banks in London are open for business;

Confidential Information: any confidential information, matter, data, know-how, documents, secrets, dealings, transactions or affairs (however recorded or preserved), whether directly or

indirectly disclosed to us by you or your employees, officers, representatives or advisers whether before, during or after the Term;

Commencement Date: 30 days from the date the Order Form is countersigned by R2C in accordance with clause 2.2;

Data: all data which a Customer uploads through the Software and any Transactions they perform;

Data Protection Legislation: the UK Data Protection Legislation and (for so long as and to the extent that the law of the European Union has legal effect in the UK) the General Data

Protection Regulation ((EU) 2016/679) and any other directly applicable European Union regulation relating to privacy;

Fees: the fees for the use of the Software and the provision of the Services set out in the

Order Form as increased from time to time in accordance with clause 8;

Information: visual, textual or other information published or otherwise made available by the Customer (directly or indirectly) using the Software;

Intellectual Property Rights: means all intellectual property rights including but not limited to the following rights existing in any party of the world: all patents, design rights, trademarks, copyright, rights in databases, trade secrets and other rights,

Confidential

Information, know-how and all other intellectual property rights of a similar nature in any part of the world, whether registered or unregistered, and all applications and the rights to apply for the protection of any of the foregoing;

Losses: losses, liabilities, damages, compensation, awards, payments made under settlement arrangements, claims, proceedings, reasonable costs and other expenses including interest and penalties, whether arising in contract, tort (including negligence), breach of statutory duty or otherwise, reasonably incurred legal and other professional fees and expenses;

Meta Data: anonymised (by removal of any components or means of identifying a specific organisation or individual in relation to certain data) aggregated Data used by R2C for the development and provision of future products and services and the performance of the Software when used by the Customer;

Minimum Term: the initial fixed minimum period of the Term, as set out in the Order Form;

Order: the Customer's offer to accept the Order Form;

Permitted Purpose: the administrative functions and processes of the Customer for their workshop or fleet management for their sole use or in conjunction with other Subscribers;

Personal Data: has the meaning set out in the Data Protection Legislation;

Order Form: R2C's order form listing the Services to be provided to the Customer;

Purpose: has the meaning given in clause 4.5(b);

Reference Data: all reference or standing data which R2C, a third party provider or a Subscriber, other than the Customer, uploads through the Software;

R2C's Service Level Agreement: the document attached hereto (where appropriate);

Renewal Term: has the meaning given in clause 11.1;

Services: the development, integration, access, hosting, Support Services, Additional Services and any other services provided by R2C in relation to the Software or as set out in the Order Form;

Service Credit: has the meaning given in clause 3.10(c);

Service Delivery Failure: has the meaning given in clause 3.10(c);

Service Hours: 9am to 5:30pm Monday to Friday (other than Bank Holidays), unless otherwise specified in the Order Form;

Service Level Arrangements: has the meaning given in clause 3.10;

Software: R2C's automated vehicle service, maintenance and repair software as a service solution as described in the Order Form and only to be accessed through R2C's web-based portal, including any error corrections, updates, upgrades, modifications and enhancements;

Subscriber: a person or organisation licensed by R2C to use the Software;

Support Services: the maintenance and support services in relation to the Software, as set out in the Order Form and R2C's Service Level Agreement;

Term: the minimum period of the Agreement until terminated in accordance with clause 11;

Trade Mark: the "R2C Online" trade mark;

Transaction: any event where the Customer creates, receives, submits, requests or transmits a record on the Software to or from another Subscriber; UK Data Protection Legislation: any data protection legislation from time to time in force in the UK including the Data Protection Act 1998 or 2018 or any successor legislation.

Uptime Service Level: has the meaning given in clause 3.10(a).

1.2 Clause headings shall not affect the interpretation of these terms and conditions.

1.3 A person includes a corporate or unincorporated body (whether or not having separate legal personality). A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established.

1.4 Words in the singular shall include the plural and vice versa.

1.5 A reference to a statute or statutory provision is a reference to it as it is in force for the time being, taking account of any amendment, extension, or re-enactment and includes any subordinate legislation for the time being in force made under it and any legislation which replaces it.

2. BASIS OF AGREEMENT

2.1 The Order Form constitutes an offer by the Customer to purchase a licence of the Software and the Services as set out in the Order Form.

2.2 The Order Form shall only be deemed to be accepted when R2C countersigns the Order Form at which point and on which date the Agreement shall come into existence.

2.3 These terms and conditions apply to the Agreement to the exclusion of any other terms that the Customer seeks to impose or incorporate, or which are implied by trade, custom, practice or course of dealing.

2.4 Any Order Form given by R2C shall not constitute an offer and is only valid for a period of 20 Business Days from its date of issue.

3. SOFTWARE AND ADDITIONAL SERVICES PROVISION

3.1 R2C grants the Customer, subject to these terms and conditions, during the Term, a worldwide, royalty-free, non-exclusive, revocable (during the Term and subject to termination in accordance with clause 11) licence for the Authorised Users, to access and, subject to 3.4, use the Software for the Permitted Purposes. The licence will terminate immediately upon termination of this Agreement for any reason.

3.2 Provided that the Customer obtains the express written consent of R2C, the Customer may sublicense any or all of its rights and obligations under this licence, subject to the Customer procuring that any proposed sub-licensee enters into a sub-licence agreement with the Customer on substantially the same terms.

3.3 The Customer agrees that it shall not and must not permit any other third party to:

- (a) duplicate, modify or distribute any portion of the Software or interfere or disrupt the Services; or

- (b) reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form any of the Software, except as may be allowed by any applicable law which is incapable of exclusion by agreement between the parties; or

- (c) modify the Software; or

- (d) use, copy or infringe the Intellectual Property Rights in relation to the Software, in order to develop any competing product, equivalent system or system components or commercially exploit the Software for any purpose other than its own core business activities.

3.4 The Customer's access to the Software, in particular the various functions of the Software shall be limited to the number of Authorised Users and level of subscription to the Software as set out in the Order Form.

3.5 In order to access the Software the Customer will be issued with a set of unique passwords. The

Customer is responsible for the security and proper use of all passwords relating to the Software and must take all necessary steps to ensure that each password is kept confidential, secure, used properly in accessing the Software and not disclosed to any party other than the relevant Authorised User. R2C may periodically require the Customer to procure that each Authorised User changes their password and shall notify the Customer accordingly.

3.6 If an Authorised User forgets misplaces or compromises any password, the Customer must contact R2C immediately and upon satisfaction of such security checks as R2C may determine, a new password will be given to enable the Software to be accessed.

3.7 The Customer must inform R2C immediately if it has any reason to believe that any password has become known to someone not authorised to use it or if any password is being or is likely to be used in an unauthorised way.

3.8 The monitoring and control of user log-ins and passwords relating to use of the Software by Authorised Users for the processing of Transactions is solely the responsibility of the Customer.

3.9 Subject to clause 3.10 the Software shall be available in accordance with the Uptime Service Level.

3.10 Unless the Customer agrees a separate Service Level Agreement with R2C the Software and any Additional Services shall be provided by R2C as follows:

(a) R2C shall provide at least a 95% uptime Software availability per month (Uptime Service Level). This availability refers only to an access point on the R2C's nominated host backbone network, as the Customer is responsible for its own internet access. Availability does not include maintenance events, Customer-caused outages or disruptions, or outages or disruptions attributable in whole or in part to force majeure events within the meaning of clause 13;

(b) R2C gives no guarantee that the Software and/or the Services will uninterrupted or error-free but R2C agrees to use reasonable endeavours to correct reported faults as soon as R2C reasonably can. Faults must be reported by the Customer to R2C by telephone (0114 399 2430), electronic mail (support@r2conline.com) or in writing to the address set out at the beginning of these terms.

(c) if availability falls below the Uptime Service Level in a given calendar month (Service Delivery Failure), R2C shall credit the Customer's account by an amount calculated as the product of the total cumulative downtime (expressed as a proportion of the total possible uptime minutes in the month concerned) and the monthly subscription Fee paid by the Customer (Service Credit);

(d) a Service Credit shall not be payable unless the Customer requests it within 30 days of the service affecting event(s). The maximum Service Credit allowable in a given month is limited to the total Fees paid by the Customer in respect of such month.

3.11 R2C reserve the right to suspend access to the Software or refuse provision of the Services in accordance with clause 9.

3.12 Subject to 3.11, R2C agrees to provide the Customer with the Services on these terms and conditions.

3.13 R2C shall supply the Software and Additional Services described in the Order Form to the Customer in accordance with any timings set out therein.

3.14 R2C shall:

(a) use its reasonable skill and endeavours in relation to the provision of the Software;

(b) co-operate with the Customer in all matters relating to the Agreement, and comply with all reasonable

instructions of the Customer;

(c) only use personnel who are suitably skilled and experienced to perform the tasks assigned to them, and in sufficient numbers to ensure that R2C's obligations are fulfilled;

(d) where the provision of the Software is paid for on a time and materials basis, ensure that the personnel who provide the Software are no more senior (and therefore no more expensive) than is appropriate, and devote no more time than is appropriate, to such performance;

(e) ensure that it obtains, and maintains all consents, licences and permissions (statutory, regulatory, contractual or otherwise) it may require and which are necessary to enable it to comply with its obligations in the Agreement;

(f) ensure that the Software and any Additional Services shall conform in all respects with the applicable description thereof set out in the Order Form and that any service levels set out in the Service Level Arrangements, shall be fit for any purpose that the Customer expressly makes known to R2C in the Order Form;

(g) comply with all Applicable Law from time to time in force, and the mandatory policies set out in the policies schedule to these Terms and Conditions.

(h) where applicable, observe all health and safety rules and regulations and any other reasonable security requirements that apply at any of the Customer's premises from time to time and are notified to R2C;

(i) notify the Customer as soon as practicable of any health and safety incidents or material health and safety hazards at any sites owned or occupied by any member of the Customer group (or any contractor thereof) of which it becomes aware and which relate to or arise in connection with the performance of the Agreement;

(j) instruct R2C personnel to adopt any necessary associated safety measures in order to manage the material health and safety hazards referred to in (h) immediately above;

(k) comply with all other obligations imposed on it as set out in the Agreement;

4. DATA PROTECTION SHARING AND SECURITY

4.1 Both parties will comply with all applicable requirements of the Data Protection Legislation. This clause

4 is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection

Legislation. In this Clause 4, Applicable Laws means (for so long as and to the extent that they apply to

R2C) the law of the European Union, the law of any member state of the European Union and/or Domestic

UK Law; and Domestic UK Law means the UK Data Protection Legislation and any other law that applies

in the UK.

4.2 The parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the

data controller and R2C is the data processor (where Data Controller and Data Processor have the meanings as defined in the Data Protection Legislation). Table 1 below sets out the subject matter, nature and purpose of processing by R2C, the duration of the processing and the types of Personal Data and categories of data subjects.

.....
.....
.....

4.3 Without prejudice to the generality of Clause 4.1, the Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to R2C for the duration and purposes of this Agreement.

4.4 Without prejudice to the generality of Clause 4.1, R2C shall, in relation to any Personal Data processed in

connection with the performance by R2C of its obligations under this Agreement:

(a) process that Personal Data only on the written instructions of the Customer unless R2C is required by

Applicable Laws to otherwise process that Personal Data. Where R2C is relying on Applicable Laws as

the basis for processing Personal Data, R2C shall promptly notify the Customer of this before performing

the processing required by the Applicable Laws unless those Applicable Laws prohibit R2C from so

notifying the Customer;

(b) ensure that it has in place at all times appropriate technical and organisational measures, reviewed and

approved by the Customer:

(i) to prevent and protect against unauthorised or unlawful processing of Personal Data and against

accidental loss or destruction of, or damage to, Personal Data, which are appropriate to the harm that

might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and

the nature of the data to be protected, having regard to the state of technological development and the

cost of implementing any measures (those measures may include, where appropriate, pseudonymising

and encrypting Personal Data);

(ii) to ensure confidentiality, integrity, availability and resilience of its systems and services;

(iii) to ensure availability of and access to Personal Data can be restored in a timely manner after an incident;

and

(iv) to provide for regular assessment and evaluation of the effectiveness of the technical and organisational

measures adopted by it;

(c) ensure that all personnel who have access to and/or process Personal Data are obliged to keep the

Personal Data confidential and are subject to legally binding confidentiality obligations;

(d) not transfer any Personal Data outside of the European Economic Area unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:

- (i) the Customer or R2C has provided appropriate safeguards in relation to the transfer;
- (ii) the data subject has enforceable rights and effective legal remedies;
- (iii) R2C complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
- (iv) R2C complies with reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;

(e) assist the Customer, at the Customer's cost, in responding to any request from a data subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to requests from data subjects, security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

(f) notify the Customer without undue delay on becoming aware of a Personal Data breach;

(g) at the written direction of the Customer, delete or return Personal Data and copies thereof to the Customer at any time and on termination of the agreement unless required by Applicable Law to store the Personal Data; and

(h) maintain complete and accurate records and information to demonstrate its compliance with this clause 4, which it shall make available to the Customer upon the Customer's reasonable written request to allow the Customer to audit such compliance.

4.5 The Customer consents to R2C appointing a third-party processor of Personal Data under this Agreement provided that:

- (a) R2C has notified the Customer of such third-party processor in writing;
- (b) R2C confirms that it has entered or will enter (as the case may be) into a written agreement with the third-party processor incorporating terms which are substantially similar to those set out in this clause 4;
- (c) upon termination of this Agreement for any reason, all Personal Data held by the third-party processor shall be deleted or returned to the Customer at the written direction of the Customer, and
- (d) as between the Customer and R2C, R2C shall remain fully liable for all acts or omissions of any third-party processor appointed by it pursuant to this clause 4.

4.6 Either party may, at any time on not less than 30 days' notice, revise this clause 4 by replacing it with any applicable controller to processor standard clauses or similar terms.

4.7 R2C will collect Meta-Data about the Customer when they register for the Software, and when the Customer uses the Software and transmits Data. The Customer expressly agrees that R2C and any member of the group of companies of which R2C is a member may use such Meta-Data for analysis and product development.

4.8 The Customer agrees that R2C may collate Meta-Data in relation to the use of the Software in order to

provide analysis and reports for the further development of the Software, and the benefit of Customers, Subscribers and third parties. R2C will use cookies to collect such information. More information about the cookies R2C shall use and how to recognise them can be found in our cookies policy. The Customer hereby expressly agrees to R2C's use of cookies.

4.9 The Customer agrees that its Data, Reference Data and Information shall be made available to other Subscribers of the Software who the Customer has authorised by the "invitation" function of the Software, and the Customer grants an irrevocable licence to R2C to use the Data for such purposes.

4.10 The Customer warrants to R2C that it does not intend to transfer Personal Data under the Agreement but should the Data, Reference Data or Information the Customer inputs into the Software contain Personal Data, then the Customer warrants that it will comply with the Data Protection Legislation if and to the extent the Data, Reference Data or Information it inputs into the Software contains or will contain Personal Data that the Customer has complied with all its requirements under the Data Protection Legislation during the continuance of the Term.

4.11 The Customer warrants and undertakes to R2C that it:

- (a) the Personal Data has been obtained and processed lawfully;
- (b) the use of the Personal Data will be entirely consistent with any appropriate specified and lawful purposes for which the Customer has registered under the Data Protection Legislation in respect of the Personal Data ("Purpose");
- (c) the Customer will not use or disclose the Personal Data in any part in a matter incompatible with that Purpose;
- (d) the Personal Data is adequate, relevant and not excessive in relation to the Purpose;
- (e) the Personal Data is accurate and the Customer will keep the Personal Data fully up to date at all times during the continuance of the Term.

4.12 R2C cannot guarantee and shall not be responsible for the accuracy, completeness or currency of any Reference Data, over which it has no control, and the Customer hereby waives any rights that it may have to make any claims against R2C in respect of the quality or quantity of the Reference Data.

4.13 R2C and the Customer undertake to each other to comply at all times with the Data Protection Legislation.

The parties shall provide one another any reasonable assistance required to comply with their obligations under the Data Protection Legislation.

4.14 The Customer hereby agrees to indemnify R2C on demand in full and shall hold R2C harmless against all actions, claims, demands, liabilities, damages, costs, losses or expenses incurred or suffered by R2C as

result of any breach by the Customer of its obligations under the Data Protection Legislation.

4.15 R2C (or its hosting provider) shall perform scheduled back-ups, provide routine and emergency data recovery, and manage the archiving process of the Data.

4.16 In the event of any loss or damage to the Data, the Customer's sole and exclusive remedy shall be for R2C to restore the lost or damaged Data from the latest back-up maintained by R2C in accordance with the archiving and recovery procedure referred to in clause 4.15, provided that R2C has fully complied with clause 4.15.

4.17 R2C shall not be responsible for any loss, destruction, alteration or disclosure of Data caused by any third party except third-party processors appointed in accordance with clause 4.5 and those third parties sub-contracted by R2C to perform services related to maintenance and back-up of the Data or to the extent resulting from R2C's failure to comply with its obligations under this Agreement including in relation to security of Data.

5. PROPRIETARY RIGHTS

5.1 The Customer acknowledges and agrees that R2C and/or its licensors own all Intellectual Property Rights in the Software, the Services and any other programs, coding, algorithms, software or other solutions developed by R2C. Except as expressly stated, these terms and conditions do not grant the Customer any rights to R2C's Intellectual Property Rights.

5.2 R2C confirms that it holds all the rights in relation to the Software that are necessary for to comply with these terms and conditions.

5.3 The Customer must:

- (a) notify R2C as soon as reasonable possible if it becomes aware of any infringement of its Intellectual Property Rights;
- (b) give R2C sole conduct of the defence, claim or action brought by a third party in respect of any purported Intellectual Property Rights infringement;
- (c) not at any time admit liability or otherwise attempt to settle or compromise claim or action brought by any third party in respect of any Intellectual Property Rights infringement, except upon R2C's express instructions; and
- (d) act in accordance with the reasonable instructions of R2C and give such assistance that R2C shall reasonably require in respect of conduct of the defence of a claim or action brought by any third party in respect of any Intellectual Property Rights infringement.

5.4 R2C shall have no liability to the Customer in respect of any Intellectual Property Right infringement to the extent the same is due to any unauthorised alterations, modification or adjustment to the Software by

the Customer without R2C's consent.

5.5 The Data is the property of the Customer and the Customer reserves all Intellectual Property Rights which may, at any time, subsist in the Data. The Meta-Data is the property of R2C and R2C reserves all

Intellectual Property Rights which may, at any time, subsist in the Meta-Data.

6. THE SERVICES

6.1 R2C shall provide the Support Services during the Service Hours.

6.2 To enable R2C to deliver the Software (and any Additional Services), the Customer shall:

- (a) provide R2C with all necessary co-operation and information in relation to the Agreement;
- (b) comply with all technical instructions published by R2C from time to time;
- (c) comply with all applicable laws and regulations with respect to its activities under these terms (including the Data Protection Legislation); and
- (d) carry out all other Customer responsibilities set out in these terms and conditions in a timely and efficient manner.

6.3 R2C may, at its sole discretion and by express agreement, agree to provide the Customer with all or any of the Additional Services at a cost to be agreed by R2C, which shall be charged to the Customer as Additional Charges.

6.4 R2C warrants and represents that it shall use all reasonable commercial endeavours to:

- (a) comply with all applicable laws in performing its obligations under the Agreement;
- (b) deliver the Software (and any Additional Services) using reasonable skill and care;
- (c) meet the Uptime Service Level set out in clause 3.10.

6.5 R2C does not warrant, nor gives any guarantee that:

- (a) the Software will operate without interruption or error or to be free of problems; or
- (b) that any Reference Data is at any time up to date or accurate; or
- (c) that the Software (or the Additional Services (if it agrees to provide them)) will not cause the Customer's other hardware or software to operate without interruption or error, or to be free of problems.

6.6 All clauses warranties terms and undertakings implied statutory or otherwise in respect of the performance by R2C of the Software are hereby excluded.

7. CUSTOMER OBLIGATIONS

7.1 The Customer is responsible for providing suitable telecommunication services, internet connections, hardware and software necessary to enable access to the Software to the minimum specification stipulated by R2C from time to time.

7.2 The Customer must not use the Software:

- (a) fraudulently or in connection with a criminal offence;
- (b) to send, receive, upload, download, use or re-use any material which is offensive, abusive, indecent, defamatory, obscene or menacing, or in breach of copyright, confidence, privacy or any other rights;

(c) to cause annoyance, inconvenience or needless anxiety whether to R2C, any other Subscriber or any other third party by any means including using the Software for persistently sending requests for information, other than as may be necessary or appropriate in respect of genuine Transaction, generating unacceptable levels of data import or failing to monitor and respond to communications;

(d) to send unsolicited advertising or promotional material;

(e) other than in accordance with the acceptable use policies of any connected networks; or

(f) in a way, whether knowingly or otherwise, which would impair the operation of the Software or put them in jeopardy.

7.3 The Customer warrants that:

(a) the Information and Data provided by the Customer (whether stored on or sent via the Software) will not contain any material which is (or the accessing of which) would be obscene, offensive, defamatory or a criminal offence or otherwise unlawful;

(b) all necessary licences and consents (including those from any third party owners or licensors) have been obtained and that the Customer will comply with all legislation, instructions or guidelines issued by regulatory authorities, relevant licensors and any other codes of practice which relate to Information or Data or are applicable or relevant to the Customer's business.

7.4 The Customer is expressly responsible for the creation, maintenance, design and configuration of all Information, Data or other material that is transmitted through the Software and the Customer must ensure that contact details are included in a clear and legible form sufficient for receipt of any enquiries or complaints regarding Information, Data or any other material which the Customer transmits through the Software. The Customer expressly acknowledges that R2C has the right to disclose such contact details to any person with an enquiry or complaint if they are unable to locate those details.

Subject matter of processing

Customer Data

Nature & Purpose of processing

The provision of the Software by R2C under the Agreement.

Duration of the processing

The Term of the Agreement and any Renewal Term if applicable.

Types of personal data

Names, email addresses and phone numbers of Customer

personnel and Customer personnel

Categories of data subject

Customer personnel & Customer personnel

TABLE 1

R2C Online: Terms & Conditions

.....
.....
.....

7.5 The Customer agrees to notify R2C immediately of any changes to the information, including but not limited to its contact details, that it provided when registering for the Software, and warrants that all information supplied at the time the Customer registered for the Software and any changes notified to those details will be true, complete and accurate in all respects.

7.6 The Customer expressly agrees that access to Reference Data is provided for the sole provision of effecting Transactions through the Software and cannot be used for any other purposes.

7.7 The Customer agrees not to use, copy or infringe the Intellectual Property Rights in relation to the Software, and any other programs, coding, algorithms, software or other solutions developed by R2C during the Term in order to develop any competing product, equivalent system or system components.

7.8 The Customer agrees to indemnify on demand R2C and keep R2C indemnified fully and effectively against all actions, proceedings, claims, demand, damages and costs (including legal costs on a full indemnity basis) incurred by R2C as a result of any breach of the warranties set out in this clause 7.

8. FEES

8.1 The Customer shall pay the Fees (and time shall be of the essence for all such payments), as set out in the Order Form.

8.2 All amounts and Fees stated or referred to in the Agreement are exclusive of value added tax, which shall be added to R2C's invoice(s) at the appropriate rate.

8.3 At any time during the Minimum Term, R2C shall be entitled to increase its Fees, provided that:

- (a) only one such increase is made in any 12 month period;
- (b) R2C give the Customer 30 days' prior notice of such increase;
- (c) such increase does not exceed the increase in the CPI published by the National Statistics Office;
- (d) At any time during a Renewal Term, R2C shall be entitled to increase its Fees, provided that it shall give the Customer 30 days' prior notice of such increase.

8.4 The Fees shall be invoiced by R2C and paid by the Customer at least 30 days prior to the Commencement Date and each period as set out in the Order Form.

8.5 R2C shall be entitled to levy Additional Charges:

- (a) if Additional Services are provided in circumstances where any reasonably skilled and competent IT engineer would have judged the Customer's request to have been unnecessary;
- (b) if the Additional Services are required as a result of any default of the Customer in compliance with its obligations under these terms and conditions or as a result of the Customer's failure to comply with R2C's reasonable instructions or directions issued from time to time; and/or

(c) if R2C shall provide any Additional Services at the written request of a duly authorised person representing the Customer for this purpose.

8.6 Additional Charges shall be levied by R2C monthly in arrears and shall be payable by the Customer within 30 days of receipt of a valid invoice. Where such an invoice is disputed, R2C will issue an invoice for any undisputed amount and the Customer agrees to pay the undisputed within 30 days of receipt of the undisputed invoice.

8.7 Interest shall accrue on overdue amounts at the rate of 4% over the base lending rate of R2C's bankers in the UK from time to time, commencing on the due date and continuing until fully paid, whether before or after the judgment.

8.8 All payments due by the Customer to R2C shall be made without set off or counterclaim.

8.9 The Customer acknowledges that R2C has the right to instigate normal credit checks if it, in its sole discretion, deems this to be appropriate and to disclose details and these terms to a credit reference agency for the purpose of assisting with credit decisions and fraud prevention. R2C reserves the right to refuse, without reason, any payment method tendered.

9. SUSPENSION

9.1 The Customer acknowledges that R2C at its absolute discretion may temporarily suspend access to the Software or the provision of the Additional Services:

(a) if R2C has not received payment by the due date and having notified the Customer of such non-payment, the Customer has failed to pay the outstanding sums owing under clause 8 within 10 Business Days of such reminder, until such payment is received, together with any accrued interest in accordance with clause 8.7; and

(b) for contravention by the Customer of clauses 3, 4, 7 and 8 and in such instance R2C will not restore access to the Software until it receives an adequate assurance from the Customer that there will be no further contravention.

9.2 R2C may from time to time temporarily withdraw, or make alterations to the Software or to the Additional Services for technical, security, maintenance and other operational reasons. R2C shall use all reasonable endeavours to give the Customer reasonable advance notice of any such downtime or alterations, but the Customer acknowledges and agrees that on occasion such downtime or alterations, for technical, security maintenance and other operational reasons, may have to be made on very short notice, or without notice. R2C shall use its reasonable endeavours to minimise any negative impact of

such changes upon the delivery of the Software or the Additional Services, and upon the Customer's business, and will wherever reasonably possible seek to avoid any reduction in core functionality of the Software and the Additional Services.

10. LIMITATION OF LIABILITY

10.1 This clause 10 sets out the entire financial liability of R2C (including any liability for the acts or omissions

of its employees, agents and sub-contractors) to the Customer in respect of:

(a) any breach of these terms and conditions;

(b) any use made by the Customer of the Software, the Additional Services, the Reference Data or any part

of them; and

(c) any representation, statement or tortious act or omission (including negligence) arising under or in

connection with these terms and conditions.

10.2 Except as expressly provided in these terms and conditions, all warranties, statements, terms and

conditions or undertakings which may be implied by statute, common law, custom or trade or otherwise

are hereby excluded to the fullest extent permitted and this clause 10 specifies the entire liability of R2C

including liability for negligence.

10.3 Except as expressly and specifically provided in these terms and conditions the Customer assumes sole

responsibility for results obtained from the use of the Software and the Additional Services by the

Customer, and for conclusions drawn from such use. R2C shall have no liability for any damage caused

by errors or omissions in any Information provided to R2C by the Customer in connection with the

Software, or any actions taken by R2C at the Customer's direction.

10.4 The Customer must tell R2C immediately if any third party makes or threatens to make any claim or

issue legal proceedings against the Customer relating to the use of the Software and the Customer will,

upon request, immediately stop the act or acts complained of. If R2C asks, the Customer must confirm the

details of the claim(s) in writing.

10.5 Use of the Software to purchase products or services from another Subscriber is solely at the risk of the

Customer and R2C shall accept no liability in respect of such products or services. In such event the

Customer will enter into a contract directly with appropriate Subscriber and not with R2C. Such order will

be subject to such conditions as that Subscriber specifies in relation to those products or services. R2C

does not monitor the content of Subscriber's websites or their terms and conditions and any links are

provided for convenience only.

10.6 Nothing in these terms and conditions excludes the liability of R2C:

(a) for death or personal injury caused by R2C's negligence; or

(b) for fraud or fraudulent misrepresentation.

10.7 The Service Level Arrangements set out in clause 3.10 state the Customer's full and exclusive right and remedy, and R2C's only obligation and liability in respect of, the performance and/or availability of the Software, or their non-performance and non-availability.

10.8 Subject to clause 10.6 and clause 10.7:

(a) R2C shall not be liable for any loss of profits, loss of business, depletion of goodwill and/or similar losses or pure economic loss, or for any special, indirect or consequential loss costs, damages, charges or expenses however arising; and

(b) R2C's total aggregate liability in contract, tort (including negligence or breach of statutory duty), misrepresentation, restitution or otherwise, arising in connection with the performance or contemplated performance of these terms and conditions shall be limited to the Fees paid to R2C by the Customer during the 12 month subscription period during which the claim arose.

11. TERM AND TERMINATION

11.1 The Agreement shall commence on the Commencement Date and, unless terminated earlier in accordance with these terms and conditions, shall continue for the Minimum Term.

11.2 After the expiry of the Minimum Term, the Agreement shall continue on a rolling 12 month term ("the Renewal Term"), unless either party serves 12 months written notice of termination upon the other party

11.3 If the Customer terminates the Agreement during the Minimum Term or any Renewal Term in accordance with clause 11.4 other than as a result of a material breach of these terms by R2C then the Customer shall pay to R2C on demand an amount equal to any and all Fees and Additional Charges that it would have paid to R2C pursuant to clause 8 calculated from the date of termination until the end of the Minimum Term or Renewal Term.

11.4 Without prejudice to any of the rights or remedies to which the parties may be entitled, the Agreement may be terminated immediately by notice in writing:

(a) by either party if the other party is in material or continuing breach of any of its obligations under the

Agreement and fails to remedy the same (if capable of remedy) within 30 days of receipt of a written notice of the breach by the other party;

(b) by R2C if the Customer fails to pay any outstanding sums after R2C issues a reminder in accordance with clause 9.1;

(c) by either party, if an order is made or a resolution is passed for the winding up of the other party, or circumstances arise which entitle a court of competent jurisdiction to make a winding-up order in relation to the other party;

(d) by either party, if an order is made for the appointment of an administrator to manage the affairs, business

and property of the other party, or documents are filed with a court of competent jurisdiction for the

appointment of an administrator of the other party, or notice of intention to appoint an administrator is

given by the other party or its directors or by a qualifying floating charge holder (as defined in paragraph

14 of Schedule B1 to the Insolvency Act 1986);

(e) by either party, if a receiver is appointed of any of the other party's assets or undertaking, or if

circumstances arise which entitle a court of competent jurisdiction or a creditor to appoint a receiver or

manager of the other party, or if any other person takes possession of or sells the other party's assets;

(f) by either party, if the other party makes any arrangement or composition with its creditors, or makes an

application to a court of competent jurisdiction for the protection of its creditors in any way, or becomes

bankrupt;

(g) by either party, if the other party ceases, or threatens to cease, to trade; or

(h) by either party, if the other party takes or suffers any similar or analogous action in any jurisdiction in

consequence of debt.

11.5 On termination:

(a) all licences granted under the Agreement shall immediately terminate;

(b) R2C may destroy or otherwise dispose of any of the Data in its possession unless R2C receives, no later

than ten days after the effective date of the termination or expiry of the Agreement, a written request for

the delivery to the Customer of the then most recent back-up of the Data. R2C shall use reasonable

commercial efforts to deliver the back-up to the Customer within 30 days of its receipt of such a written

request, provided that the Customer has, at that time, paid all Fees, Additional Charges and any sums

outstanding at and resulting from termination (whether or not due at the date of termination). The

Customer shall pay all reasonable expenses incurred by R2C in preparing a copy of the Data; and

(c) the accrued rights of the parties as at termination, or the continuation after termination of any provision

expressly stated to survive or implicitly surviving termination, shall not be affected or prejudiced.

11.6 For the avoidance of doubt, until the Data is destroyed, all licences granted by the Customer to R2C in

respect of the Data shall survive termination of these terms.

12. VARIATIONS TO THE AGREEMENT

Subject to clause 8.3 and clause 1.5, no variation, modification, addition, supplement or other change to these terms shall be effective unless in writing and signed by duly authorised representatives of each of the parties.

13. FORCE MAJEURE

R2C shall have no liability to the Customer under these terms and conditions if it is prevented from or delayed in performing its obligations under these terms and conditions, or from carrying on its business,

by acts, events, omissions or accidents beyond its reasonable control, including, without limitation,

strikes, lock-outs or other industrial disputes (whether involving the workforce of R2C or any other party),
failure of a utility service or transport network, act of God, war, riot, civil commotion, malicious damage,
compliance with any law or governmental order, rule, regulation or direction,
accident, breakdown of plant
or machinery, fire, flood, storm or default of suppliers or subcontractors provided that the Customer is notified of such an event and its expected duration.

14. CONFIDENTIALITY

14.1 Each party may be given access to Confidential Information from the other party in order to perform its obligations under these terms and conditions. A party's Confidential Information shall not be deemed to include information that:

- (a) is or becomes publicly known other than through any act or omission of the receiving party; or
- (b) was in the other party's lawful possession before the disclosure; or
- (c) is lawfully disclosed to the receiving party by a third party without restriction on disclosure; or
- (d) is independently developed by the receiving party, which independent development can be shown by written evidence; or
- (e) is required to be disclosed by law, by any court of competent jurisdiction or by any regulatory or administrative body.

14.2 Subject to clause 4.3, each party shall hold the other's Confidential Information in confidence and, unless required by law, not make the other's Confidential Information available to any third party or use the other's Confidential Information for any purpose other than the implementation of the Agreement.

14.3 This clause 14 shall survive termination of the Agreement, however arising.

15. NOTICES

15.1 Any notice required to be given under these terms and conditions shall be in writing and shall be delivered by hand or sent by pre-paid first-class post or recorded delivery post to the other party at its registered office address, or such other address as may have been notified by that party for such purposes.

R2C Online: Terms & Conditions

.....
.....
.....

15.2 A notice delivered by hand shall be deemed to have been received when delivered (or if delivery is not in business hours, at 9 am on the first Business Day following delivery). A correctly addressed notice sent by pre-paid first-class post or recorded delivery post shall be deemed to have been received at the time at which it would have been delivered in the normal course of post.

16. GENERAL

16.1 A waiver of any right under these terms and conditions is only effective if it is in writing and it applies only to the party to whom the waiver is addressed and to the circumstances for which it is given.

16.2 Unless specifically provided otherwise, rights arising under these terms and conditions are cumulative and do not exclude rights provided by law.

16.3 If any provision (or part of a provision) of these terms and conditions is found by any court or administrative body of competent jurisdiction to be invalid, unenforceable or illegal, the other provisions shall remain in force.

16.4 If any invalid, unenforceable or illegal provision would be valid, enforceable or legal if some part of it were deleted, the provision shall apply with whatever modification is necessary to give effect to the commercial intention of the parties.

16.5 These terms and conditions and any documents referred to in them, constitute the whole agreement between the parties and supersede any previous arrangement, understanding or agreement between them relating to the subject matter they cover.

16.6 Each of the parties acknowledges and agrees that in entering into the Agreement it does not rely on any undertaking, promise, assurance, statement, representation, warranty or understanding (whether in writing or not) of any person (whether party to the Agreement or not) relating to the subject matter of the Agreement, other than as expressly set out in the Agreement.

16.7 The Customer shall not, without the prior written consent of R2C, assign, transfer, charge, subcontract or deal in any other manner with all or any of its rights or obligations under these terms and conditions.

16.8 R2C may at any time assign, transfer, charge, sub-contract or deal in any other manner with all or any of its rights or obligations under these terms and conditions.

16.9 Nothing in these terms and conditions is intended to or shall operate to create a partnership between the parties, or authorise either party to act as agent for the other, and neither party shall have the authority to act in the name or on behalf of or otherwise to bind the other in any way (including, but not limited to, the making of any representation or warranty, the assumption of any obligation or liability and the exercise of any right or power).

16. 10 The Agreement is made for the benefit of the parties to it and (where applicable) their successors and permitted assigns, and is not intended to benefit, or be enforceable by, anyone else.

17. GOVERNING LAW AND JURISDICTION

17.1 These terms and conditions and any disputes or claims arising out of or in connection with their subject matter are governed by and construed in accordance with the laws of England.

17.2 The parties irrevocably agree that the courts of England have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with these terms and conditions.

R2C Online: Terms & Conditions

.....
.....
.....

Highways England

Fleet Management Software

Service Information Final

September 2019

Revised March 2020

Table of Contents

1. General.....	3
2 General Requirements	5
3 Service Specification	7
4 IT Specification	8
5 Constraints on how the Service Provider provides the Service	18
6 Mobilisation.....	25
7 Services and other things provided by the Customer.....	25
8 Property affected by the service.....	25
9 Health and Safety.....	25
Appendix A – Live Data Transfer.....	27
Appendix B – Management Information	30
Appendix C – Data Protection	32
Appendix D – Secure data handling requirements.....	34
Appendix E – Data Security Standard	Error! Bookmark not defined.
Appendix F – Non-functional requirements	38

1. General

1.1 Introduction and Background

1.1.1 Highways England is charged with operating, maintaining and improving England's motorways and major A roads. In order to do this, Highways England operate a varied fleet of vehicles across three distinct operational units:

- Traffic Officer Vehicles (TOV) – currently comprising of 240 Highways England-owned vehicles based across 39 operational out stations across the country, managed by the Vehicles Team in Birmingham. These vehicles operate 24/7/365 responding to incidents on the countries Strategic Road Network (SRN).
- Asset Delivery (AD) Vehicles – currently comprising of 175 Highways England-owned vehicles across multiple operational sites, managed by the Vehicles Team in Birmingham. These vehicles operate 12 hours/day inspecting the condition of the assets on the countries SRN. The number of vehicles within this fleet is expected to rise to 275 by 2021.
- Winter Fleet Vehicles – currently comprising of 437 vehicles across 100 operational sites. Vehicles are owned by Highways England but operated and maintained by third party service delivery contractors across 14 Areas. Fleet performance is tracked by a central Winter Team in Birmingham. This fleet responds during period of adverse weather to maintain flow across the SRN.

1.1.2 Across the three areas a significant amount of data relating to servicing, maintenance and vehicle utilisation is collected. Data is currently managed through a number of teams and stored in a variety of formats including multiple software applications. The result is an inability to easily and reliably identify trends, fulfil long term vehicle renewal goals, compile operational and financial reports consistently and provide up to date accurate management information.

1.1.3 The scope of this project is to procure and deliver a central cloud-based fleet management system via the provision of Software as a Service. Collating core data for all vehicle types within the Highways England fleet into one central system should provide easy access to accurate data allowing pro-active economic fleet management decisions to be made.

1.2 Duration

1.2.1 This Contract will be for a duration of two years.

1.3 Objectives

1.3.1 The *Customer's* objectives are to:

- Increase accessibility, consistency, efficiency and clarity of all information relating to their fleet of vehicles across the business
- Harness data to improve pro-active fleet management decision-making. This includes but is not limited to the ability to:
 - Understand vehicle utilisation by vehicle make, model and type both regionally and nationally
 - Reduce vehicle off road (VOR) time.
 - Identify vehicle whole life cost & vehicle history.
 - Maximise vehicle resale value through holding comprehensive service and maintenance records
 - Schedule all required vehicle maintenance events including servicing and MOT
 - Configure dashboard reporting to analyse, monitor and manage real time fleet performance and metrics
 - Identify trends and systemic issues to inform proactive preventative maintenance programmes
 - Comprehensively respond to vehicle and part recalls under manufacturer's warranty, as well as avoid costs when vehicles and / or parts are still under warranty
 - Build a comprehensive database of information to inform future vehicle replacement programmes.

2 General Requirements

2.1 Financial Management

- 2.1.1 The *Service Provider* includes on invoices the requisition number and, where appropriate, the purchase order number. The *Service Provider* submits with each invoice such records as the *Customer* requires.
- 2.1.2 The *Service Provider* notifies the *Customer* of the name and address of his bank, the account name and number, the bank sort code and any other details required to make direct payments into that account.
- 2.1.3 The *Customer* will require one invoice/month for all Goods and Services and licence costs from the *Service Provider*.

2.2 Contract Management

- 2.2.1 The *Service Provider* shall attend reviews every 3 months as organised by the *Customer*. The meetings shall be held at the *Customer's* premises unless otherwise agreed. The *Service Provider's* Account Manager would be expected to attend or to delegate as appropriate when unable to attend.
- 2.2.2 The *Customer* expects the *Service Provider* to manage/support the transfer from current software providers at the start and end of the contract period as required by the *Customer*
- 2.2.3
- 2.2.5 The *Service Provider* is expected to provide the capability to interface with current systems and integrate data according to open standards as cited in the Gov.UK Technology Code of Practice:
<https://www.gov.uk/guidance/gds-api-technical-and-data-standards>

2.3 Equality and diversity

- 2.3.1 The *Service Provider* must comply with the requirements of the *Customer's* Equality, Diversity and Inclusion ambition to embed the principles of equality, diversity and inclusion into all areas of our business, driving real change in how we work with our *Customers* and communities, our supply chain and our employees and the Equality Act 2010. The *Service Provider* must pay due regard to the connection between equality, diversity and inclusion, engagement and wellbeing.

2.3.2 The *Service Provider* must:

- Acknowledge that the *Customer* views each area of diversity as being important and consequently that the *Customer* intends to proactively promote all areas of diversity; and
- Ensure that no individual is treated less favourably because of their connection with any protected characteristic as detailed in the Equality Act 2010 or any legislation which supersedes this.

2.3.3 The *Service Provider's* on-line platform should comply with Web Content Accessibility Guidelines WCAG2.1 AA accessibility standard and must be accessible and inclusive for the needs of all *Customer's* employees who have access to the platform.

3 Service Specification

3.1 General

3.1.1 In line with the service level agreement and platform service specification attached. The *Service Provider* will be able to provide the functionality marked with a tick below. Items marked with a cross are outside of scope for phase 1. Subsequent development to deliver these would be subject to scope, product steering group approval and would incur additional costs.

ID	Requirement	Theme	Response
1	Cloud-based software	Functional Requirements	Yes
2	Capable of holding records for up to 2,500 individual vehicles	Functional Requirements	Yes
3	Accessible across multiple operational sites	Functional Requirements	Yes
4	Accessible across multiple hardware platforms, including mobile	Functional Requirements	Yes
5	Capable of interfacing automatically with multiple data feeds detailed in Appendix A – Live Data Transfer	Functional Requirements	Yes
6	Compliance with all data transfer requirements detailed in Appendix A – Live Data Transfer	Data Capture	Yes
7	Configurable dashboard reporting to incorporate all elements of data within Appendix B – Management Information	Reporting	Yes - requires VP and once set can be configured via Dev - VP V2 will allow for user configuration
8	Compliance with management information requirements as detailed in Appendix B – Management Information	Reporting	Yes
9	Provision of telephone support during standard working hours of 09:00 to 17:30 Mon – Fri	Support	With changes
10	E-ticket system available outside the core hours stated above	Support	Yes
11	Action plan for resolving support queries to be provided within the limits set out in the attached SLA	Support	Yes
12	Account Manager for duration of the contract	Support	Yes
13	Data migration of current vehicle data securely from multiple data sources, whilst mitigating risk of potential loss of data	Implementation	Yes
14	Training provided for all users	Implementation	Yes

15	Provision of project manager to oversee the installation and on-boarding process	Implementation	Yes
16	Hosted securely in line with ISO/IEC 27001 requirements	Security / Audit	Yes
17	Deliver all detailed non-functional Highways England requirements as referred to in Appendix F – Non-Functional Requirements	Non-Functional Requirements	Yes

IT Specification

4.1 Service Definition

- 4.1.1 The *Service Provider* shall deliver and maintain over the term of the Agreement all software products necessary to provide the capability to monitor, manage and maintain Highways England’s fleet of vehicles.
- 4.1.2 The *Service Provider* shall ensure inclusion of requisite standard industry software, and service components.
- 4.1.3 The *Service Provider* shall provide required documentation associated with the managed service, this includes but is not limited to, training materials and administration guidance sheets.

4.2 Functional Design

- 4.2.1 The *Service Provider* shall deliver a comprehensive functional design for the managed service platform which shall include developing a solution model that fully articulates the features and requirements of the specification. This is restricted to the items outlined in the table in 3.1.1.
- 4.2.2. The *Customer’s* Non-Functional Requirements (NFR) for the system are detailed in Appendix F.

4.3 Technical Design

- 4.3.1 The *Service Provider* shall provide a comprehensive technical design which will deliver the non-functional requirements and service levels. This design will include, but not be limited to:

- Access available via a web-based portal - Google Chrome (version 72.0.3636.121), Mozilla Firefox (version 52.3.0) and/or MS IE 11 or later.
- Data is to be stored in the UK
- The Customer has the ability to ensure no new personal or sensitive data is to be added to the *Customer's* systems.
- The ability to interface with other Customer's systems is required. Details of current systems with which data interface is required are provided in Appendix A – Data Transfer
- Web Services are encrypted to the standard required by the Customer's Cyber Security specification – see Section 4 for Cyber specification.

4.4 Cyber Security requirements:

The *Service Provider* shall have in place the required standards and security to provide appropriate protection for the *Customer's* data. These standards and systems will include but not be limited to:

- ISO/IEC 27001 Certified

4.4.1 Should the Service Provider deploy all or part of the solution into a Cloud Environment e.g. Microsoft Azure, Amazon AWS or Google Cloud. The NCSC 14 Cloud Security Principles shall be implemented.

4.4.2 The Service Provider shall comply with the following Highways England Information Security documents which governs the movement and storage of data and legislative requirements:

- Secure Data Handling Requirements – Appendix D
- Data Security Standard – In the Service Level Agreement

4.4.3 Not Used

4.4.4 Inventory and Control of Software Assets

- Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organisation's authorised software inventory. Unsupported software should be tagged as unsupported in the inventory system
- Ensure that unauthorised software is either removed or updated in a timely manner.

4.4.5 Continuous Vulnerability Management

- Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor
- Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.

4.4.6 Controlled Use of Administrative Privileges

- Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts
- Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

4.4.7 Maintenance, Monitoring and Analysis of Audit Logs

- Ensure that local logging has been enabled on all systems and networking devices.

4.4.8 Email and Web Browser Protections

- Ensure that only fully supported web browsers and email clients are allowed to execute in the organisation, ideally only using the latest version of the browsers and email clients provided by the vendor
- The Customer's preferred browser is Google Chrome, followed by Firefox.
- Use Domain Name System (DNS) filtering services to help block access to known malicious domains.

4.4.9 Malware Defences

- Utilise anti-malware software to continuously monitor and defend each of the organisation's workstations and servers
- Ensure that the organisation's anti-malware software updates its scanning engine and signature database on a regular basis.

4.4.10 Limitation and Control of Network Ports, Protocols, and Services

- Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

4.4.11 Data Recovery Capabilities

In line with the r2c Service Level agreement

- Ensure that all system data is automatically backed up on a regular basis
- Ensure that all of the organisation's key systems are backed up
- Ensure that backups are properly protected via encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services
- Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination
- Ensure that the backup period is configurable.

4.4.12 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

- Install the latest stable version of any security-related updates on all network devices.

4.4.13 Boundary Defence

- Maintain an up-to-date inventory of all of the organisation's network boundaries.
- Deny communication over unauthorised TCP or UDP ports or application traffic to ensure that only authorised protocols are allowed to cross the network boundary in or out of the network at each of the organisation's network boundaries.

4.4.14 Separation between users

- A malicious or compromised user of the Cloud Service should not be able to affect the service or data of another.

4.5 Software Configuration

4.5.1 The *Service Provider* shall provide implementation services for the Fleet Management Managed Service which shall include:

- configuration of the software and other software components to produce an integrated solution from a user perspective
- configuration of the software and other software components to support the requirements of the specification

4.6 Testing

4.6.1 The Service Provider shall carry out testing for the service platform in accordance with paragraphs 4.6.2 through 4.6.8 inclusive, including the following as required:

- test strategy, this should be available as soon as possible and within 15 working days of the contract start date
- test planning, this should be available as soon as possible and within 15 working days of the contract start date
- an enumerated list of test requirement and definitions
- engineering and running unit and component tests
- engineering and running integration and end-to-end tests
- engineering and running regression tests
- engineering and running user acceptance and usability tests
- engineering and running operational acceptance tests
- engineering and running load, performance and stress tests
- test exception and issue resolution
- test reporting
- “penetration testing”
- security testing of data visibility – who sees what and when
- plugins/ Interface testing.

4.6.2 The test strategy must include:

- an overview of how testing will be conducted in relation to the implementation plan (the implementation plan is to be produced by the Service Provider no later than 15 days after the contract start date)
- the procedure to be followed to ensure that testing is performed by an individual independent of the system development team
- the process to be used to capture and record test results and the categorisation of test issues
- the procedure to be followed should a deliverable (any software or document to be used by the Customer) fail a test or where a deliverable produces unexpected results, including a procedure for the resolution of test issues
- the procedure to be followed to sign off each test; and
- the process for the production and maintenance of reports relating to tests.

4.6.3 The test planning must include:

- For the application, the high-level system service objectives a statement that the product meets those objectives
- For each enumerated business requirement of the application, a detailed procedure for each test to be carried out, including expected result,

method of testing, timescales, production and access for Customer to test reports

- the mechanism for ensuring the quality and relevance of tests
- the retest schedules.

4.6.4 Testing shall be undertaken on the ability to connect, navigate, successfully use the offering, and to report out of the offering on standard devices the Customer wishes to test. Standard devices mean laptops, desktops and mobiles (tablets and phones) within the Customer's IT infrastructure i.e. with the Customer's builds and behind firewalls and various Government orientated security features. Testing shall also cover the same type of devices external to the Customer's IT infrastructure.

4.6.5 Testing shall be undertaken on the transfer of data back to the Customer by means agreed with the Customer. The testing shall evidence that the desired data is successfully transferred in a suitable and usable format for the Customer.

4.6.6 Testing shall be planned and coordinated with the Customer. Any defects or bugs shall be recorded by the Service Provider and fixed to the satisfaction of the Customer which shall not be reasonably withheld. Any testing internal to the Service Provider does not require the Customer's involvement. This shall be carried out in line with the r2c Online Service Level agreement

4.6.7 The Customer expects the Service Provider to include testing costs associated with the testing.

4.7 Implementation and roll out

4.7.1 The Service Provider shall provide implementation and roll out services which shall ensure "right first-time" deployment to business as usual (BAU) users of the managed service platform to support the business of the Customer. As a minimum requirement, the Service Provider must facilitate:

- collaborative working with the Customer
- handover to the Customer
- documenting and training in operational procedures to be undertaken by the Customer

- deployment services
- cut over services
- readiness services, to prepare for cut over to live operations, of hardware, software, data, users and operational services
- stabilisation.

4.7.2 The Service Provider shall provide an implementation plan no later than 15 days after the start of the contract commencement day. The contract commencement date will be up to maximum of 30 days following the signing of the Order Form

- 4.7.3 Within the agreed cost the The Customer expects the Service Provider's software system to have the ability to interface with software currently in use. Please see Appendix A for a list of current software from which data will need to be migrated. Any development of interfaces which do not currently exist would be subject to an additional scope, product steering group sign-off and potential additional cost.
- 4.7.4 The Service Provider's fleet management platform should have the ability to receive all relevant data transferred from the Customer by this means or other arrangements as agreed with the Customer.
- 4.7.5 Upon receipt of data, the Customer expects the Service Provider to integrate data provided into the fleet management platform within five working days of receipt.
- 4.7.6 The Service Provider's fleet management platform should have the capability to integrate with the Customer's ITIL Service Management processes.

4.8 Data Services

- 4.8.1 The *Service Provider* shall provide data services for the service platform which shall include, data reporting services, data validation services and data export facilities.
- 4.8.2 In the event that the *Service Provider* can no longer provide the service platform for any reason, including bankruptcy, the *Service Provider* should make provision for the *Customer's* information to be transferred to the *Customer* in in an open format such as CSV, JSON or XML within 30 days of the inability to provide the contracted service.

4.9 Training Services

- 4.9.1 The *Service Provider* shall provide generalised and specialised training for their platform to those parties identified by the *Customer* as users of the platform. This shall include standard training materials and training data (to simulate operating conditions). The maximum number of individuals to be trained is ten.
- 4.9.2 The *Customer* requires the *Service Provider* to provide costs for additional user training should extra training be required outside that included as part of

initial system implementation. The cost for Additional Services are included in the Order Form.

4.10 Operational Service

4.10.1 Operational services apply to the whole term of the agreement following deployment and shall support the on-going business as usual service platform.

4.10.2 The Service Provider shall provide operational services in relation to the managed service platform which shall include:

- hosting services to provide application environments
- application management, maintenance and development
- network services and management, WAN (Wide Area Network) & LAN (Local Area Network)
- security services and management
- backup and restore
- disaster recovery service
- connectivity services
- end to end service management
- first, second and third line support services
- service desk
- incident management
- problem management
- remedial maintenance
- change management
- release and deployment management
- capacity management
- licence management
- availability management
- service level management
- request management
- service management support including monitoring, measuring and reporting of the operational services to the service levels.

4.11 Disaster recovery

4.11.1 In line with the included Service Level Agreement, the *Service Provider* must have a robust business continuity and disaster recovery plan in place on the commencement date of the contract.

- 4.11.2 The *Service Provider* must provide separate business continuity and disaster recovery plans. These should be reviewed every 6 months or after any major incident.
- 4.11.3 The *Service Provider* must have a robust business continuity plan in place to maintain the delivery of services during periods of unplanned unavailability of the online platform and/or offline service(s).
- 4.11.4 The *Service Provider* shall maintain its readiness with a business continuity plan in accordance with the principles and operation of ISO27001.
- 4.11.5 The *Service Provider* shall provide a comprehensive disaster recovery plan which details the processes by which significant disruptions will be managed to support the *Customer* and users in the event of disruptions of significant scale and impact.
- 4.11.6 If in the event of an emergency or crisis management situation, as defined within the business continuity and disaster recovery plan produced by the *Service Provider*, the *Service Provider* shall notify the *Customer* immediately, and within 4 hours. The details of the *Service Provider* process for the management of the potential emergency shall be clearly defined in the business continuity and disaster recovery plan.
- 4.11.7 The *Service Provider* must have a mechanism for testing the business continuity and disaster recovery plan on a regular basis (and in any event not less than once in every contract year). The *Service Provider* shall also perform a test of the business continuity and disaster recovery plan in the event of any major reconfiguration of the goods and/or services or as otherwise reasonably requested by the *Customer*.
- 4.11.8 The *Service Provider* shall not delete or remove any proprietary notices contained within or relating to the *Customer's* data. The *Service Provider* shall not store, copy, disclose, or use the *Customer's* data except as necessary for the performance by the *Service Provider* of its obligations or as otherwise approved by the *Customer*.
- 4.11.9 The *Service Provider* shall take responsibility for preserving the integrity of *Customer's* data and preventing the corruption or loss of *Customer* data.
- 4.11.10 The *Service Provider* shall perform secure back-ups of all the *Customer's* data and shall ensure that up-to-date back-ups are stored off-site at an approved location within the UK in accordance with any BCDR Plan or otherwise.
- 4.11.11 The *Service Provider* shall ensure that such back-ups are available to the *Customer* (or to such other person as the *Customer* may direct) at all times upon request.

- 4.11.12 The *Service Provider* shall ensure that any system on which the *Service Provider* holds any *Customer* data, including back-up data, is a secure system that complies with the Security requirements.
- 4.11.13 If at any time the *Service Provider* suspects or has reason to believe that the *Customer* data is corrupted, lost or sufficiently degraded in any way for any reason, then the *Service Provider* shall notify the *Customer* immediately and inform the *Customer* of the remedial action the *Service Provider* proposes to take.

4.12 Service Desk

- 4.12.1 The *Service Provider* shall provide a service desk. The service desk shall be the support route for users experiencing issues with the managed service. The service desk must be accessible via a range of channels including but not limited to a web-site (with FAQs), e-mail, and phone for both portable and desk top configurations as agreed with the *Customer*.

5 Constraints on how the Service Provider provides the Service

5.1 Information security

- 5.1.1 The *Service Provider* acknowledges that the *Customer* places great emphasis on the confidentiality, integrity and availability of information and consequently on the security of all elements of the *Service Provider's* Service.
- 5.1.2 The *Service Provider* shall at all times provide a level of security which is in accordance with Good Industry Practice (in relation to any particular circumstances, the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading expert provider of services or supplier of goods, within the relevant industry or business sector, performing services or supplying goods substantially similar to the Services or goods to customers of the same size and nature as the Customer.) and this Agreement;
- 5.1.3 The *Customer* retains the right to audit the delivery of the Services and the Contract at any time, in line with the '*Customer* Audit Procedure'
- 5.1.4 Systems should adhere to the relevant Cyber Security best practice guidance for the technology area. This includes:
- Web-based systems must protect against the OWASP top 10, and should follow the principles of the NCSC architecture pattern for Serving Web Content its child documents.
 - Cloud-based systems must follow NCSC's Cloud Security Principles.
- 5.1.5 Passwords must be changed from defaults, and reject known and weak passwords
- 5.1.6 The *Service Provider* must agree an incident reporting process with the *Customer* for security incidents and flaws. This process will include tracking the issue and the progress against any corrective action plan.
- 5.1.7 The *Service Provider* must report incidents and flaws within 24 hours of discovery.
- 5.1.8 The *Service Provider* must draw up a corrective action plan within 24 hours of the initial reporting of the flaw/incident.
- 5.1.9 Any security incident classified as a major incident shall be subject to root cause analysis. The major problem review report for such problems shall document the cause, along with any remedial action which could prevent a recurrence and shall be issued to the *Customer*.

5.2 Data Protection

Definitions

- **Data** is all Personal Data collected, generated or otherwise processed by the *Service Provider* in the course of Providing the Service.
- **Data Protection Acts** are:
 - the General Data Protection Regulation (EU2016/679) and the Data Protection Act 2018
 - at all times, any other data protection laws and regulations applicable in England and Wales.
- **Data Subject** is an individual who is the subject of Personal Data.
- **EEA** is the European Economic Area
- **Personal Data** is any data relating to an identified or identifiable individual that are within the scope of protection as “personal data” under the Data Protection Acts.
- **Security Incident** is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Data.
- **Supervisory Authority** is any regulatory, supervisory, governmental or other competent authority with jurisdiction or oversight over the Data Protection Acts. The UK Supervisory Authority is the Information Commissioner’s Office.

5.2.1 For the purposes of this contract and the Data Protection Acts

- the *Customer* is the Data Controller for employee data shared with the *Service Provider*
- the *Service Provider* is the Data Processor for the employee data shared by the *Customer*
- this section and Appendix C Data Protection, together, constitute a data processing agreement where required by the Data Protection Acts.

5.2.2 The *Service Provider* processes the Data in accordance with the Data Protection Acts and only to the extent necessary for the purpose of Providing the Service.

5.2.3 The *Service Provider* does not knowingly do anything or permit anything to be done which might lead to a breach of the Data Protection Acts by either Party.

5.2.4 The *Service Provider* obtains and maintains throughout the Service Period all registrations and notifications that it is obliged to obtain and maintain pursuant to the Data Protection Acts in respect of Providing the Service.

- 5.2.5 Without prejudice of 5.2 the *Service Provider* processes the Data only in accordance with the instructions of the *Customer*, unless the *Service Provider* is required to process Data for other reasons under the laws of the European Union (or a member state of the EEA) to which the *Service Provider* is subject. If the *Service Provider* is required to process the Data for these other reasons, it informs the *Customer* before carrying out the processing, unless prohibited by relevant law.
- 5.2.6 The *Service Provider* immediately informs the *Customer* if it believes that an instruction infringes the Data Protection Acts or any other applicable law.
- 5.2.7 The *Service Provider* has in place and maintains for as long as it holds any Data in accordance with then current good industry practice, taking into account the state of the art, the costs of implementing and the nature, scope, context and purposes of processing:
- appropriate technical and organisational measures (having regard to the nature of the Data) to protect the Data against accidental, unauthorised or unlawful processing, destruction, loss, damage, alteration or disclosure and
 - adequate security programmes and procedures to ensure that unauthorised persons do not have access to the Data or to any equipment used to process the Data.

In each case to ensure that the *Service Provider's* processing is in accordance with the Data Protection Acts and protects the rights of Data Subjects.

- 5.2.8 The *Service Provider* ensures that all persons authorised to process Data are bound by obligations equivalent to those set out in this section and are aware of the *Service Provider's* obligations under the contract and the Data Protection Acts.
- 5.2.9 The *Service Provider* ensures access to the Data is limited to those persons who need access in order for the *Service Provider* to Provide the Service under the contract and (in each case) to such parts of the Data as are strictly necessary for performance of that person's duties.
- 5.2.10 Where the *Service Provider* obtains or collects Personnel Data on behalf of the *Customer*, the *Service Provider*:
- provides to Data Subjects a data protection notice in a form accepted by the *Customer* informing the Data Subject of the identity of the *Service Provider*, the identity of any data protection representative it may have appointed, the purpose or purposes for and legal basis upon which their Personal Data will be processed and any other information which is necessary having regard to the specific circumstances in which the Personal Data is, or is to be, processed to enable processing in respect of the Data Subject to be fair and

- where applicable, obtains all necessary consents for the processing of Data.
- 5.2.11 On request, the *Service Provider*, takes all necessary actions and provides the *Customer* with all reasonable assistance necessary for the *Customer* to comply with its obligations under the Data Protection Acts in relation to the rights of Data Subjects, including:
- the provision of access to, and information relating to, Data
 - the rectification of inaccurate Data
 - the permanent erasure of Data
 - the restriction of processing of Data
 - the provision of a copy of Data in machine readable format, and
 - the transfer of Data to a third party.
- 5.2.12 The *Service Provider* immediately notifies the *Customer* if it receives:
- a request from any Data Subject whose Personal Data it holds to access their Personal Data
 - a complaint or request relating to the *Customer's* obligations under the Data Protection Acts, or
 - a request from any Supervisory Authority for assistance or information, unless provided by relevant law.
- 5.2.13 The *Service Provider* assists and co-operates with the *Customer* in relation to any complaint or request received, including:
- providing full details of the complaint or request
 - complying with the request within the time limits set out in the Data Protection Acts and in accordance with the instructions of the *Customer*, and
 - promptly providing the *Customer* with any Personal Data and any other information requested by it to enable it to respond to the request.
- 5.2.14 The *Service Provider* does not process the Data outside the EEA (other than in the United Kingdom) without the agreement of the *Customer*. Where the *Customer* agrees, the *Service Provider*:
- provides evidence (acceptable to the *Customer*) of appropriate safeguards as required by the Data Protections Acts and
 - complies with the instructions of the *Customer*.
- 5.2.15 The *Service Provider* complies with the requirements of the *Customer* in relation to the storage, dispatch and disposal of Data in any form or medium. Any requirement for the *Service Provider* to destroy or delete copies of the Data is subject to any law of the European Union (or a member state of the EEA) to which the *Service Provider* is subject that requires Data to be retained.

- 5.2.16 The *Service Provider* notifies the *Customer* within 24 hours of becoming aware of a Security Incident or any other breach of this section. The notification includes, as far as possible:
- a description of the nature of the Security Incident, including the categories and approximate number of Data Subjects concerned
 - the likely consequences of the breach and
 - the measures taken, or to be taken, to address the breach, including measures taken to mitigate any possible adverse effects.
- 5.2.17 In the event of a Security Incident, the *Service Provider* provides the *Customer* with full co-operation and assistance in dealing with the Security Incident, in particular in notifying individuals affected by the Security Incident or a Supervisory Authority as required by the Data Protection Acts.
- 5.2.18 On request (but not more than once in any 12 month period) the *Service Provider* provides to the *Customer* all necessary information to demonstrate the *Service Provider's* compliance with this section.
- 5.2.19 The *Service Provider* promptly provides all assistance and information requested by any Supervisory Authority or required by the *Customer* in order for the *Service Provider* to ensure compliance with its obligations under the Data Protection Acts, including in relation to:
- security of processing,
 - preparation of any necessary data protection impact assessments and
 - undertaking any necessary data protection consultations.
- 5.2.20 The *Service Provider* maintains electronic records of all processing activities carried out on behalf of the *Customer*, including:
- the information described in this section
 - the different types of processing being carried out (if applicable),
 - any transfers of Data outside of the EEA or the United Kingdom, identifying the relevant country or international organisation and any documentation required to demonstrate suitable safeguards and
 - a description of the technical and organisational security measures referred to in this section.
- The *Service Provider* makes these records available to the *Customer* promptly on request.
- 5.2.21 If it is or becomes a requirement that, under the Data Protection Acts or other applicable laws, this section must be governed by the laws of a member state of the European Union, and the law of the contract does not or ceases to satisfy this requirement, this section is governed by and construed in accordance with the laws of Ireland.

5.2.22 A failure to comply with this section is treated as a substantial failure by the *Service Provider* to comply with its obligations.

5.3 Service Provider's Premises, access and storage to *Customer's* data

5.3.1 Any Risk Assessment is carried out by the *Customer* in accordance with a risk assessment method agreed with the *Customer's* IT Security team and the Cabinet Office Policy: Offshoring information assets classified at OFFICIAL document, version 1.1 dated November 2015, or any later revision or replacement.

5.3.2 Except as expressly specified otherwise in this contract, the *Service Provider* provides all premises necessary to Provide the Service.

5.3.3 The *Service Provider* does not use any premise to Provide the Service until

- the premise has successfully passed the Risk Assessment. The *Customer* may request the *Service Provider* to provide any information required to support any Risk Assessment or
- the *Customer* has confirmed that a premise does not require to be assessed in accordance with the Risk Assessment.

5.3.4 The *Service Provider* provides the *Customer* with any information required to support any Risk Assessment.

5.3.5 The *Service Provider* does not store any of the *Customer's* data that is classified as Official or higher in accordance with "Government Security Classifications" dated April 2014 (or any later revision or replacement):

- offshore or
- in any way that it could be accessed from an Offshore location until the *Customer* has confirmed to the *Service Provider* that either
- the *Customer* has gained approval for such storage in accordance with "Offshoring information assets classified at OFFICIAL" dated November 2015 (or any later version or replacement)
- or such approval is not required.

5.3.6 The *Service Provider* complies with a request from the *Customer* to provide any information required to allow the *Customer* to gain approval for storing data or allowing access to data from an Offshore location in accordance with this clause.

5.4 Conflict of Interest

5.4.1 The *Service Provider* does not take an action which would cause a conflict of interest to arise in connection with this contract. The *Service Provider* notifies the *Customer* if there is any uncertainty about whether a conflict of interest may exist or arise.

5.4.2 The *Service Provider* notifies his employees that they do not take an action which would cause an actual or potential conflict of interest to arise in connection with the *service*. The *Service Provider* immediately notifies the *Customer* if there is any uncertainty about whether a conflict of interest may exist or arise.

5.4.3 If the *Service Provider* notifies the *Customer* of a conflict of interest, the *Customer* may:

- require the *Service Provider* to stop Providing the Service until any conflict of interest is resolved
- require the *Service Provider* to submit to the *Customer* for acceptance a proposal to remedy the actual or potential conflict of interest.

5.4.4 A reason for not accepting the submission is that it does not resolve any conflict of interest. The *Service Provider* amends the proposal in response to any comments from the *Customer* and resubmits it for acceptance by the *Customer*. The *Service Provider* complies with the proposal once it has been accepted.

- any step taken under this condition is not a compensation event
- A failure to comply with this condition is treated as a substantial failure by the *Service Provider* to comply with his obligations.

5.5 Discrimination

5.5.1 The *Service Provider* does not discriminate directly or indirectly or by way of victimisation or harassment against any person contrary to the Equality Act 2010, any predecessor statute of it or any amendment or re-enactment of it from time to time (the "Discrimination Acts").

5.5.2 In Providing the Service, the *Service Provider* co-operates with and assists the *Customer* to satisfy its duty under the Discrimination Acts to eliminate unlawful discrimination and to promote equality of opportunity between persons of different racial groups and between disabled people and other people.

5.5.3 Where any employee of the *Service Provider* is required to carry out any activity alongside the *Customer's* employees in any premises, the *Service Provider* ensures that each such employee complies with the *Customer's* employment policies and codes of practice relating to discrimination and equal opportunities.

5.5.4 The *Service Provider* notifies the *Customer* in writing as soon as he becomes aware of any investigation or proceedings brought against the *Service Provider* under the Discrimination Acts in connection with this contract and:

- provides any information requested by the investigating body, court or tribunal

- attends (and permits a representative from the *Customer* to attend) any associated meetings
- promptly allows access to any relevant documents and information and
- cooperates fully and promptly with the investigating body, court or tribunal.

5.5.5 The *Service Provider* indemnifies the *Customer* against all costs, charges, expenses (including legal and administrative expenses) and payments made by the *Customer* arising out of or in connection with any investigation or proceedings under the Discrimination Acts resulting from any act or omission of the *Service Provider* or any of his staff.

5.5.6 A failure to comply with this requirement is treated as the *Service Provider* having substantially failed to Provide the Service.

6 Mobilisation

6.1 The *Customer* requires a mobilisation plan for commencement of Services, this is requested as part of the quality submission.

6.2 The *Supplier* shall within 60 working days from the start of the Contract deliver to the *Customer* an Exit Plan which sets out the *Supplier's* proposed methodology or achieving an orderly transition of Information and Services to the *Customer* and or a Replacement Supplier.

7 Services and other things provided by the Customer

7.1 The *Customer* will provide Data so that the *Service Provider* can provide the services.

7.2 The *Customer* works in the spirit of mutual trust and cooperation.

8 Property affected by the service

8.1 The *Service Provider* carries out basic security checks on his employees before they are involved in Providing the Service. The checks are carried out in accordance with the *Customer's* procedures.

9 Health and Safety

9.1 The *Service Provider* complies with the *Customer's* rules, regulations, health and safety policies and any safety and security instructions notified to the *Service Provider*.

- 9.2 The *Service Provider* reports to the *Customer* any accidents to people employed by the *Service Provider* which require to be reported in accordance with relevant health and safety legislation.
- 9.3 The *Service Provider* and the *Customer* notify each other of any known special health and safety hazards which may affect the performance of the services. The *Service Provider* informs and instructs people employed by him on the hazards and any necessary associated safety measures.
- 9.4 The *Service Provider* complies with *Customer's* Interim Advice Note 128/15AR Highways England Supply Chain Health and Safety Incident Reporting ("IAN 128"), or its later update or replacement, including any time periods required by IAN 128. If no time period is specified in IAN 128 the period of reply applies unless agreed otherwise by the *Customer*.
- 9.5 If any incident occurs that the *Service Provider* considers is not within the remit of IAN 128 the *Service Provider*:
- notifies the *Customer* of the incident and
 - reports the incident as if the incident was in the remit of IAN 128 if required by the *Customer*

Appendix A – Live Data Transfer

1. Data Transfer

Data to be transferred from the *Customer* to the *Service Provider* via ongoing interface / upload will include but not be limited to:

Data to be transferred and held in system		Data Transfer Frequency				Data transfer source (<i>and format</i>)		
ID	Data	One-Off	Annual	Ad Hoc	Daily	TOV & AD	WF pre 2018	WF post 2018
1	Vehicle Registration Number	x				BT Qlik (.csv)	SWIS ¹	Exactrak ²
2	Fleet ID Number	x				BT Qlik (.csv)	SWIS	Exactrak
3	Vehicle Type	x				BT Qlik (.csv)	SWIS	Exactrak
4	Vehicle Make & Model	x				BT Qlik (.csv)	Winter Team (.csv)	
5	Chassis Number	x				BT Qlik (.csv)	Winter Team (.csv)	
6	Key Codes	x				BT Qlik (.csv)	Not required	Not required
7	Radio Codes	x				BT Qlik (.csv)	Not required	Not required
8	Axel Weight	x				BT Qlik (.csv)	SWIS	Exactrak
9	Operational Base	x				BT Qlik (.csv)	SWIS	Exactrak
10	Operational Area	x				BT Qlik (.csv)	SWIS	Exactrak
11	Operational Region	x				BT Qlik (.csv)	SWIS	Exactrak

¹ Severe Weather Information Service (SWIS) is a bespoke system recording information for pre - 2018 vehicles.

² Exactrak records data including real time tracking, location, and gritter efficiency for winter fleet vehicles. Weekly reports are provided via a link to the Exactrak server.

Specification

ID	Data	One-Off	Annual	Ad Hoc	Daily	TOV & AD	WF pre 2018	WF post 2018
12	Vehicle Warranty	x				BT Qlik (.csv)	Not available	Winter team (.csv)
13	Vehicle Insurance renewal date		x			BT Qlik (.csv)	Regional M&R contractor	
14	Vehicle tax renewal date		x			BT Qlik (.csv)	Winter team (.csv)	
15	MOT date		x			BT Qlik (.csv)	Not required	Not required
16	Vehicle service date		x			BT Qlik (.csv)	Not required	Not required
17	Vehicle maintenance event			x		BT Qlik (.csv)	Regional M&R contractor	
18	Vehicle parts / repair warranty			x		BT Qlik (.csv)	Regional M&R contractor	
19	Vehicle Off Road periods			x		BT Qlik (.csv)	Exactrak	Exactrak
20	Driver endorsements			x		Future Requirement	Not required	
21	Driver licenses			x		Future Requirement	Not required	
22	Vehicle mileage at start / end shift / journey				x	Masternaut/ L&A (.csv)	SWIS	Exactrak
23	Fuel Card transactions				x	TMC (API)	Not required	Not required
24	Vehicle mileage at refuel				x	TMC (API)	Not required	Not required
25	GPS data for each vehicle per journey				x	Masternaut/ L&A (.csv)	SWIS	Exactrak
26	Pre-Drive checks				x	Future Requirement	Not required	Not required
27	Driver details per shift				x	Future Requirement	Not required	Not required

Specification

ID	Data	One-Off	Annual	Ad Hoc	Daily	TOV & AD	WF pre 2018	WF post 2018
28	Vehicle idling time				x	Masternaut/ L&A (.csv)	Not required	Not required
29	Amber light usage				x	Masternaut/ L&A (.csv)	Not required	Not required

Appendix B – Management Information

Management Information available to the *Customer* from the *Service Provider's* on-line platform.

1.1 General requirements

The *Customer* expects managers and budget holders to have instant access to a configurable dashboard of information through the *Service Provider's* platform to include but not be limited to:

ID	Report	TOV & AD	WF
1	Current fleet availability	✓	✓
2	Total, average and maximum vehicle utilisation per time period	✓	✓
3	Total, average and maximum time spent in outstations / workshops per time period	✓	✓
4	Number of vehicles with future maintenance events in the next four weeks	✓	✗
5	Future service, maintenance and MOT events within the next four weeks	✓	✗
6	Future service, maintenance and MOT events outside the next four weeks	✓	✓
7	Odometer readings	✓	✓
8	Fuel card transactions	✓	✗
9	Fuel consumption & spend per time period	✓	✓
10	Driver details per shift	✓	✗
11	Speeding events over 70 MPH for longer than 20 seconds per time period	✓	✗
12	Pre-Drive Check completion	✓	✗
13	Vehicle departure and arrival times at outstation / depot	✓	✓
14	Total number of vehicle trips per time period	✓	✗
15	Total number of vehicle miles driven per time period	✓	✗
16	Total, average and maximum miles driven per trip	✓	✓
17	Total, average and maximum idling time per time period	✓	✓
18	Total, average and maximum idling time at outstation / depot per time period	✓	✓
19	Total, average and maximum amber light usage per time period	✓	✗
20	Vehicle off Road (VOR) - estimated completion time to deal with reported issue and manage VOR time and incidents	✓	✓
21	Live and historical vehicle defect, repair and damage details	✓	✓
22	Service and maintenance history	✓	✓
23	Total maintenance spend in period	✓	✓
24	Total financial spend per vehicle in period	✓	✓

ID	Report	TOV & AD	WF
25	Future vehicle tax events due in next eight weeks	✓	✓
26	Vehicle performance in relation to fuel spend, utilisation and maintenance spend	✓	✓
27	Calculation of carbon impact of vehicles	✓	✓
28	Current mileage per vehicle	✗	✓
29	Vehicles currently out on the network – numbers and locations	✗	✓
30	Recent routes covered	✗	✓
31	Vehicle location	✗	✓

APPENDIX C – DATA PROTECTION

Processing, Personal Data and Data Subjects

The *Service Provider* shall complete the following table as part of the mobilisation process to confirm their arrangements for the management and processing of data.

Description	Details
Subject matter of the processing	<i>Management of vehicles to ensure compliance with the DVSA.</i>
Duration of the processing	<ul style="list-style-type: none"> • <i>Personal customer data: Personal data will be held for as long as the individual is a customer of the company plus a minimum of 18 months.</i> • <i>Customer Invoice PDF: Digital invoices generated by the r2c platform, customer business information held for a minimum of 7 years.</i> • <i>Jobsheet PDF: digital jobs generated by the r2c platform, held for a minimum of 18 months.</i> • <i>Scanned documents: Non-digital documents not generated by the r2c platform but uploaded by r2c customers, no minimum retention required, deleted on request of the r2c customer.</i>
Nature and purposes of the processing	<i>The processing of customer asset (vehicle) information including asset details, work schedules, defects, organisation details and user details for the purpose of using the system to manage compliance of assets.</i>
Type of Personal Data	<p><i>Personal data processed in relation to platform users, including:</i></p> <ul style="list-style-type: none"> • <i>Names</i> • <i>E-mail addresses</i> • <i>Personal telephone numbers</i> • <i>Addresses</i> • <i>Signatures</i> • <i>Usernames</i> • <i>Personal IP Addresses</i>
Categories of Data Subject	<i>Platform users</i>
Plan for return and destruction of the data once the processing is complete UNLESS	<i>When the retention timeframe expires, r2c Online Limited will actively destroy the data as described in the r2c Online’s Data Retention Policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions</i>

<p>requirement under union or member state law to preserve that type of data</p>	<p><i>will be approved only by a member or members of r2c Online Limited 's senior management team.</i></p> <p><i>The company specifically directs users not to destroy data in violation of this policy. Destroying data that a user may feel is harmful to himself or herself or destroying data in an attempt to cover up a violation of law or company policy is particularly forbidden.</i></p>
--	--

APPENDIX D – SECURE DATA HANDLING REQUIREMENTS

Information Security Classifications

Information created and received by Highways England shall be classified according to the sensitivity of its contents. Classification and controls must take account of organisational needs for sharing or restricting information, and the associated impacts and risks, e.g. unauthorised access or damage to the information.

OFFICIAL

Description

The classification used within Highways England for all information is OFFICIAL. Information classified as OFFICIAL includes but is not limited to:

- Routine correspondence (where there is no confidentiality requirement)
- One-off exchanges with third parties
- Employee newsletters
- Internal phone directories
- Inter-office memoranda
- Internal policies and procedures
- Questions around project delivery

Impact of Compromise

Compromise of OFFICIAL information is likely to affect individual departments within Highways England and may cause local media coverage or give external attackers knowledge which could indirectly lead to a further compromise of Highways England data.

Marking

There is no requirement to explicitly mark OFFICIAL information.

Information Access

Internal and external access to Highways England data is governed by the security classification of the information which itself is derived from the government classification scheme. Which as a whole is also subject to the Freedom of Information Act.

OFFICIAL

For information classified as OFFICIAL all persons requiring access, both physical and logical must undergo appropriate employment screening checks defined in the Baseline Personal Security Standard (BPSS).

Information Transfer

Methods of Transfer

Information can be transferred in a variety of ways, both direct and indirect. These include:

- Spoken Word
- Post, fax, or e-mail
- Internet or intranet
- Portable Media (including CDs, DVDs, Memory Sticks and Data Cartridges)
- Electronic File Transfer
- Web Portals
- Print, Film, Fiche, Video, DVD Images

OFFICIAL

Highways England Information must only be transferred to persons who are authorised to have access to it. There must be adequate security measures in place at the virtual and/or physical destination. The definition of adequate is defined in the IS Data Security Standard, where a security measures adequacy is unclear guidance shall be sought from the Highways England Information Security team.

Geographical Restrictions

In all cases the route through which information travels both physically and logically shall be in accordance with the boundaries defined in the Data Security Standard (Appendix F).

Information Storage

Information shall be stored throughout its existence in an environment suited to its format and security classification, to ensure its preservation from physical harm or degradation and its security from loss or unauthorised access. Technical requirements are detailed in the Data Security Standard (Appendix F)

Physical Protection

Information in all formats should be stored in conditions that protect it from threats to its physical integrity through unnecessary wear and tear; specific threats such as fire, flooding, and magnetic fields; and environmental extremes or fluctuations. Where the information system or its data is classed as business-critical special storage equipment and environments should be used

Physical access to information should be restricted by locking it in rooms, cabinets, drawers, and other storage areas or units when not in use, and by ensuring that files and computer monitors are not left open to general or casual view.

Logical Protection

Protection from unauthorised access may require mechanisms such as password-protection or encryption of digital files and data, and sign-in sheets or request dockets for access to non-digital information.

Where information is stored on a mobile device (e.g. PDA, USB drive, laptop), special care must be taken to ensure that the device is physically protected from theft, loss, or damage, particularly if it is transferred or used away from Highways England business sites.

Storage Location

Information, whether original or duplicate, shall never be kept outside Highway England owned systems (e.g. on PC hard drives, on CDs or other removable media) except as part of a solution that Highways England has formally procured from a supplier or as a temporary off-line copy driven by an immediate business need to work off-site or off-line, or for authorised transfer to other users or systems.

Offshoring

Information shall only be kept in the geographical boundaries defined in the Data Security Standard (Appendix F). Any exception to these boundaries shall require prior agreement from Highways England Information Security.

APPENDIX E – NOT USED

APPENDIX F – NON-FUNCTIONAL REQUIREMENTS

1 GLOSSARY OF TERMS

The following provides a glossary of terms and definitions used throughout this document to ensure an understanding of language and acronyms used.

Acronym/Statement	Description
AD	Active Directory
BA	Business Analyst
BPSS	Baseline Personnel Security Standard
BU	Business User
CCS	Crown Commercial Service – an executive agency and trading fund of the Cabinet Office in the UK Government
CESG	Communications Electronics Security Group
CHECK	CHECK is defined as The CHECK scheme which enables penetration testing by CESG approved companies, employing penetration testing personnel qualified to assess IT systems for HMG and other public sector bodies.
CMDB	Configuration Management Database
Customer	For the purposes of these requirements, the Customer shall include the Customer's public sector partners, 3rd party Contractors, suppliers and delivery partners as authorised and indicated by the Customer.
DDoS	DDoS is defined as a Distributed Denial of Service, which is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack
DUNs Number	Data Universal Numbering System – the means of identifying business entities on a location-specific basis (9 digit number)
EDRMS	Electronic Document and Records Management System
EEA	European Economic Area
EU	European Union
FR	Functional Requirement
GBP	British pound sterling – official currency of the United Kingdom
IDC	Investment Decision Committee
ITIL	Information Technology Infrastructure Library
ITSCM	Information Technology Service Continuity Management
Knowledge Based Users	<p>Knowledge Based Users comprise the majority of the Customer's Users. They use the standard set of rich productivity tools to perform core activities identified in the requirements.</p> <p>Knowledge Based Users must be able to work from designated Customer Premises, and will also move between Customer Premises (excluding Outstations) or work from home on an ad-hoc basis. Knowledge Based Users are also likely to work offline using End User Devices.</p> <p>Knowledge Based Users normally work within the hours of 0700 – 1900 Monday – Friday</p>
KPI	Key Performance Indicators
NFR	Non-Functional Requirement
OBC	Outline Business Case – contains information needed in order to decide if a project should progress

PSN	Public Services Network
RIS	Road Investment Strategy – sets out the long term strategy to improve England’s motorways and major roads
RPO	Recovery Point Objective. It is the maximum targeted period in which data might be lost from an IT service due to a major incident
RTO	Recovery Time Objective. It is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption).
SaaS	Software as a Service (SaaS). The capability provided to the Customer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. Web-based email), or a program interface. The Customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings
Service	All references to 'the Service' in this Requirements Catalogue shall refer to Software as-a-Service (SaaS) and to include basic Service Integration unless otherwise stated.
Disruption to Service	An Incident that prevents users from accessing any of the services provided under the Fleet Management Software Managed Service. This includes any fault of such description that is the responsibility of the Service Provider but excludes faults outside the control of the Service Provider.
SHARE	Current Highways England internal document management system - Sharing Highways Agency Records Electronically
SMA	The Customer operates a 'Tower' model for its ICT services. Service Management Assist (SMA) is a “tower” model used to manage and oversee problem solving and change implementation across the various Towers.
SPOC	Single Point of Contact
SME	Subject Matter Expert
SSO	Single Sign-On
Supplier	The provider of the Service
UPTIME Data Centre Tier 3	The Uptime data centre standards are a standardised methodology used to determine availability in a facility. Tier 3 infers Multiple independent distribution paths serving IT equipment. Generally, only one distribution path serves equipment at any given time.
UW	User Workshop

PRIORITIES

Throughout this document each requirement has been given a priority rating using MoSCoW.

M	Must Have
S	Should Have
C	Could Have
W	Would Like but not essential

2 NON-FUNCTIONAL REQUIREMENTS

This section describes the requirements that specifies criteria that can be used to judge the operation of a system, i.e.: the "constraints", "quality attributes", "quality goals", "quality of service requirements" and "non-behavioural requirements".

The non-functional requirements are to be defined in the following categories:

NFR-LAF- 1.0	Look And Feel requirements(LAF)
NFR-UAH- 2.0	Usability and Humanity Requirements(UAH)
NFR-PRF- 3.0	Performance Requirements(PRF)
NFR-OAE- 4.0	Operational and Environment Requirements(OAE)
NFR-MAS- 5.0	Maintainability and Support Requirements(MAS)
NFR-SEC- 6.0	Security Requirements(SEC)
NFR-LEG- 7.0	Legal Requirements(LEG)
NFR-TRN- 8.0	Service Transition Requirements(TRN)
NFR-MGR-9.0	Data Migration Requirements(MGR)
NFR-EXT-10.0	Exit Planning Requirements(EXT)

2.1 Look and Feel Requirements (LAF)

BR ID:	NFR-LAF-1.0	
Functional Category:	Look and Feel Requirements (LAF)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Look and Feel Requirements	
Requirement Description:	<p>Describes the non-functional requirements regarding the way a system appears and the experience of using the system. The requirements include the following sub-categories:</p> <ul style="list-style-type: none"> NFR-LAF-1.1 – Branding 	

2.1.1 Branding

BR ID:	NFR-LAF-1.1	
Functional Category:	Look and Feel Requirements (LAF)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Branding	
Requirement Description:	<p>The System must allow for the application of Highways England corporate branding, using the styles and standards outlined in the 'Highways England – Visual Identity Guidelines'.</p>	

2.2 Usability and Humanity Requirements (UAH)

BR ID:	NFR-UAH-2.0	
Functional Category:	Usability and Humanity (UAH)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Usability and Humanity Requirements	
Requirement Description:	<p>Describes the System's ease of use and any special considerations needed for a better user experience. It covers the following requirements:</p> <ul style="list-style-type: none"> NFR-UAH-2.1 - Data Input NFR-UAH-2.2 - Email Notifications NFR-UAH-2.3 - Error Logs NFR-UAH-2.4 - Language NFR-UAH-2.5 - Time NFR-UAH-2.6 - Training NFR-UAH-2.7 - Warning Notifications NFR-UAH-2.8 - Accessibility NFR-UAH-2.9 - Health and Safety 	

2.2.1 Data Input

BR ID:	NFR-UAH-2.1	Originator/Source:	
Functional Category:	Usability and Humanity (UAH)	Priority:	S
Status:	New		
Comments:			
Requirement Title:	Data Input		
Requirement Description:	Validation pick-lists shall be managed and applied as much as possible, but context-driven to ensure that only relevant pick-list information is presented to the user. Mandatory data fields shall be identified in a consistent (e.g. colour-coded) manner and a spell checker facility, selectable by the user, may be applied to free text fields.		

2.2.2 Email Notifications

BR ID:	NFR-UAH-2.2	Originator/Source:	
Functional Category:	Usability and Humanity (UAH)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Email Notifications		
Requirement Description:	The system must allow the configuration of e-mail notifications, enabling the addition, modification and deletion of e-mail recipients.		

2.2.3 Error Logs

BR ID:	NFR-UAH-2.3	Originator/Source:	
Functional Category:	Usability and Humanity (UAH)	Priority:	S
Status:	New		
Comments:			
Requirement Title:	Error Logs		
Requirement Description:	Error messages displayed to the User shall be informative and easy to understand and comprehensive error logs shall be written in enough technical detail to enable investigation to be carried out.		

2.2.4 Language

BR ID:	NFR-UAH-2.4	Originator/Source:	
Functional Category:	Usability and Humanity (UAH)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Language		
Requirement Description:	All user interfaces (including log files, audit files, number and currency) text and formatting shall be in the following languages: <ul style="list-style-type: none">• UK English		

2.2.5 Time

BR ID:	NFR-UAH-2.5	Originator/Source:	
Functional Category:	Usability and Humanity (UAH)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Time		
Requirement Description:			
All data shall be presented to an operator and user in GMT			

2.2.6 Training

BR ID:	NFR-UAH-2.6	Originator/Source:	
Functional Category:	Usability and Humanity (UAH)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Training		
Requirement Description:			
System training shall be provided to the users and administrators of the System. The training shall be able to be provided via the following mediums:			
<ul style="list-style-type: none">• Quick User Guides• Written comprehensive User Guides• System and online based• Assisting Highways England in promulgating approved advice to Users via appropriate channels (normally corporate email).• Ongoing support and guidance to the customer on an ad-hoc basis and whenever there is a significant change in functionality.			

2.2.7 Warning Notifications

BR ID:	NFR-UAH-2.7	Originator/Source:	
Functional Category:	Usability and Humanity (UAH)	Priority:	S
Status:	New		
Comments:			
Requirement Title:	Warning Notifications		
Requirement Description:			
The System must issue warnings if leaving a screen will result in loss of data.			

2.2.8 Accessibility

BR ID:	NFR-UAH-2.8	Originator/Source:	
Functional Category:	Usability and Humanity (UAH)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Accessibility		
Requirement Description:			
The Service should be able to support 3rd party accessibility software such as magnification and literacy aids.			

2.2.9 Health and Safety

BR ID:	NFR-UAH-2.9	Originator/Source:	
Functional Category:	Usability and Humanity (UAH)	Priority:	S
Status:	New		
Comments:			
Requirement Title:	Health and Safety		
Requirement Description:			
The System and Supplier shall comply with their obligations in relation to the Management of Health and Safety at Work (Amendment) Regulations 2006 for IT including any changes in legislation.			

2.3 Performance (PRF)

BR ID:	NFR-PRF-3.0	Originator/Source:	
Functional Category:	Performance (PRF)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Performance		
Requirement Description:			
Describes how fast, how safe, how efficient the functionality must be. It covers the following requirements:			
<ul style="list-style-type: none">• NFR-PRF-3.1 - Business Process Delay• NFR-PRF-3.2 - Concurrent Login• NFR-PRF-3.3 - Performance Reporting			

2.3.1 Business Process Delay

BR ID:	NFR-PRF-3.1	Originator/Source:	
Functional Category:	Performance (PRF)	Priority:	S
Status:	New		
Comments:			
Requirement Title:	Business Process Delay		
Requirement Description:			
The System must provide responses without any perceptible delay for routine business operations. Operations which do not produce an immediate response should display an appropriate message.			

2.3.2 Concurrent Login

BR ID:	NFR-PRF-3.2	Originator/Source:	
Functional Category:	Performance (PRF)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Concurrent Login		
Requirement Description:			
The System must be capable of supporting minimum 10 and up to 30 concurrent logon sessions, without detriment to overall performance. This figure can vary in accordance with the detail in the Scope.			

2.3.3 Performance Reporting

BR ID:	NFR-PRF-3.3	
Functional Category:	Performance (PRF)	Originator/Source:
Status:	New	Priority: C
Comments:		
Requirement Title:	Performance Reporting	
Requirement Description:		
The Supplier shall provide the Customer with the mechanisms to easily understand the status and performance of the System.		

2.4 Operational and Environment (OAE)

BR ID:	NFR-OAE-4.0	
Functional Category:	Operational and Environment (OAE)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Operational and Environment	
Requirement Description:		
Describes the operating environment for the System and any considerations that must be taken into account and any constraints of the operational environment. Requirements include:		
<ul style="list-style-type: none"> • NFR-OAE-4.1 – User Rights/ Roles • NFR-OAE-4.2 – Compatibility • NFR-OAE-4.3 – Interfaces • NFR-OAE-4.4 – Environmental Considerations • NFR-OAE-4.5 – Web Based Delivery 		

2.4.1 User Rights / Roles

BR ID:	NFR-OAE-4.1	
Functional Category:	Operational and Environment (OAE)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	User Rights / Roles	
Requirement Description:		
The System must support role based access control. The following requirements cover user rights and access in more depth:		
<ul style="list-style-type: none"> • NFR-OAE-4.1.1 – Internal • NFR-OAE-4.1.2 – Active Directory • NFR-OAE-4.1.3 – Internal User Restrictions • NFR-OAE-4.1.4 – Virtual Private Network • NFR-OAE-4.1.5 – Access Control 		

2.4.1.1 Internal

BR ID:	NFR-OAE-4.1.1	Originator/Source:	
Functional Category:	Operational and Environment (OAE)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Internal		
Requirement Description:			
The System must allow access to Customer users. This may be by means of user authentication. The System must allow for segregated access i.e. the role will dictate the areas open for access.			

2.4.1.2 Active Directory

BR ID:	NFR-OAE-4.1.2	Originator/Source:	
Functional Category:	Operational and Environment (OAE)	Priority:	S
Status:	New		
Comments:			
Requirement Title:	Active Directory		
Requirement Description:			
The System must ensure access to all electronic records and functionality are restricted to authorised personnel only via an Active Directory Federation aware application, supporting distributed authentication and authorisation of services.			

2.4.1.3 Internal User Restrictions

BR ID:	NFR-OAE-4.1.3	Originator/Source:	
Functional Category:	Operational and Environment (OAE)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Internal User Restrictions		
Requirement Description:			
The System must be designed in such a way that areas or components of the system can only be accessed by certain groups of users dictated by roles and responsibilities.			
Groups required, but not limited to, are:			
<ul style="list-style-type: none">• Administration• Fleet managers			

2.4.1.4 Secure Connection

BR ID:	NFR-OAE-4.1.4	Originator/Source:	
Functional Category:	Operational and Environment (OAE)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Virtual Private Network (VPN)		
Requirement Description:			
The Service should allow for secure access over HTTPS (TLS1.2) and enable information classified at OFFICIAL and OFFICIAL SENSITIVE.			

2.4.1.5 Access Control

BR ID:	NFR-OAE-4.1.5	
Functional Category:	Operational and Environment (OAE)	Originator/Source:
Status:	New	Priority: S
Comments:		
Requirement Title:	Access Control	
Requirement Description:		
<p>The Supplier shall control and secure each User's access to the functions they are entitled to use through the use of authentication and authorisation services based on an appropriate, industry standards-based directory system.</p> <p>In providing the Access Control Service the Supplier shall:</p> <ul style="list-style-type: none"> • record, log and report key events; • review the current and future provision of User profiles and categories and recommend improvement actions; • manage and monitor the use and control of privileges and privileged user; • enable the Customer to request, provision, manage and revoke privileged User and system accounts and the associated credentials; • manage User's accounts such that they have only the privileges necessary to perform their function • manage and report on breaches of privileges, attempts to subvert privileges or unauthorised attempts at accessing accounts • The Customer shall be provided with the ability to add, delete or change User accounts in accordance with Service Requests. A Service Request is an official request of the Employer for the Supplier, or vice-versa, to do something to/with the Managed Service. 		

2.4.2 Compatibility

BR ID:	NFR-OAE-4.2	
Functional Category:	Operational and Environment (OAE)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Compatibility	
Requirement Description:		
<p>The System must be accessible from a web-browser and be compatible with Edge, Google Chrome and FireFox 52.3.0 as a minimum. The system must also be compatible and accessible with operating systems that underpin the main mobile technologies including tablets and mobile phones.</p>		

2.4.3 Interfaces

BR ID:	NFR-OAE-4.3	
Functional Category:	Operational and Environment (OAE)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Interfaces	
Requirement Description:	<p>Describes the requirements for exchange of information between Oracle HR and external systems. Further details are specified in the following sub-requirements.</p> <p>An exchange of information between Oracle HR to enable Traffic Officer details to be exchanged.</p> <ul style="list-style-type: none"> • NFR-OAE-4.3.1 – Oracle Human Resources (Oracle HR) 	

2.4.4 Environmental Considerations

BR ID:	NFR-OAE-4.4	
Functional Category:	Operational and Environment (OAE)	Originator/Source:
Status:	New	Priority: S
Comments:		
Requirement Title:	Environmental Considerations	
Requirement Description:	<p>The Supplier will undertake to follow a sound environmental management policy so that its activities comply with all applicable environmental legislation and regulations and that the Services are procured, produced, delivered and are capable of being used, in ways that are appropriate from an environmental protection perspective. This covers:</p> <ul style="list-style-type: none"> • ISO 14000/14001 or equivalent certification for its environmental management and shall comply with and maintain such certification requirements throughout the Contract Period. • Obligations under Directive 2002/96/EC on Waste Electrical and Electronic Equipment and Directive 2002/95/EC on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment. • Data centre facilities an operational Power Usage Effectiveness (PUE) rating, as outlined by the Green Grid, targeting the reduction of CO2 omissions and efficient operation of infrastructure. • Energy Efficiency Directive 2012/27 EU complying with the energy efficiency standards as set out in Article 6 Annex iii of the directive 	

2.4.5 Web Based Delivery

BR ID:	NFR-OAE-4.5	
Functional Category:	Operational and Environment (OAE)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Web Based Delivery	
Requirement Description:		

The Service must be delivered to Users as web-based HTTP(s) applications which should include adaptive design to cater for multiple screen sizes on PC and mobile devices.

The Service may also be accessible via an application compatible and accessible from common desktops, laptops and mobile devices in use in the UK.

2.5 Maintainability and Support (MAS)

BR ID:	NFR-MAS-5.0	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Maintainability and Support	
Requirement Description:		
<p>Describes the requirements surrounding expected System changes and the time and process needed to make them; also the specification of the support to be given to the system. It covers the following sub-categories:</p> <ul style="list-style-type: none"> • NFR-MAS-5.1 – Document Management • NFR-MAS-5.2 – Availability • NFR-MAS-5.3 – Back-up and Recovery • NFR-MAS-5.4 – Service Design • NFR-MAS-5.5 – System Life-cycle and Support • NFR-MAS-5.6 – Data Centre • NFR-MAS-5.7 – Data Centre Location 		

2.5.1 Document Management

BR ID:	NFR-MAS-5.1	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: S
Comments:		
Requirement Title:	Document Management	
Requirement Description:		
<p>Describes the non-functional requirements relating to document management. Details covered in sub-requirements.</p> <p>For information records management will be carried out via export and storage into the Customer's Electronic Document and Record Management System:</p> <ul style="list-style-type: none"> • NFR-MAS-5.1.1 – Record Format • NFR-MAS-5.1.2 – Lock Record • NFR-MAS-5.1.3 – Record Maintenance • NFR-MAS-5.1.4 – Audit 		

2.5.1.1 Record format

BR ID:	NFR-MAS-5.1.1	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Record Format		
Requirement Description:	The System must be able to store records even if they are formed of differing formats be they email, document, spreadsheet, or other file in a hierarchical, searchable structure. The System does not need to provide records management functionality such as retention, as all records will be exported and managed by the Customer.		

2.5.1.2 Lock Record

BR ID:	NFR-MAS-5.1.2	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Lock Record		
Requirement Description:	The System must have the ability to create a record, which as a minimum should mean the ability to lock down information into a read-only format to prevent changes e.g. converting into PDF format or removing edit and delete permissions.		

2.5.1.3 Record Maintenance

BR ID:	NFR-MAS-5.1.3	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Record Maintenance		
Requirement Description:	The System must have the ability to maintain formats beyond the life of the software used to create the information e.g. maintaining the ability to open information through MIME-types.		

2.5.1.4 Audit

BR ID:	NFR-MAS-5.1.4	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Audit		
Requirement Description:	The System must provide an audit of all actions either by specific user or of actions against a document/data entry regardless of user e.g. creating, editing, opening, deleting.		

BR ID:	NFR-MAS-5.2	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: S
Comments:		
Requirement Title:	Availability	
Requirement Description:		
<p>Describes the requirements for availability of the System. It covers:</p> <ul style="list-style-type: none"> • NFR-MAS-5.2.1 – Hours of Accessibility • NFR-MAS-5.2.2 – Maintenance and Remedial Activity • NFR-MAS-5.2.3 – Availability • NFR-MAS-5.2.4 – Hours of support 		

2.5.2.1 Hours of Accessibility

BR ID:	NFR-MAS-5.2.1	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: S
Comments:		
Requirement Title:	Hours of Accessibility	
Requirement Description:		
<p>The system must be accessible 24/7, but with business/support hours being 08:00 to 18:00 Monday to Friday excluding bank holidays.</p>		

2.5.2.2 Maintenance and Remedial Activity

BR ID:	NFR-MAS-5.2.2	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: S
Comments:		
Requirement Title:	Maintenance and Remedial Activity	
Requirement Description:		
<p>The Supplier shall schedule preventive maintenance to the system including, without limiting, patches; upgrades; system changes and remedial work outside of normal business hours (08:00-18:00), except in exceptional circumstances and with the agreement of the Customer.</p> <p>In the unlikely event that the Customer needs to make changes as a result, the Supplier must provide advanced notice to be agreed by the Customer.</p>		

2.5.2.3 Availability

BR ID:	NFR-MAS-5.2.3	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: S
Comments:		
Requirement Title:	Availability	
Requirement Description:		
<p>The Supplier must provide at least 98% availability for the Service at all times.</p>		

2.5.2.4 Hours of Support

BR ID:	NFR-MAS-5.2.4	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Hours of Support	
Requirement Description:	The Supplier must provide support for the Service within normal UK business hours, 09:00-17:30, Monday to Friday excluding Bank Holidays.	

2.5.3 Back-Up and Recovery

BR ID:	NFR-MAS-5.3	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Back Up and Recovery	
Requirement Description:	<p>Describes the non-functional requirements relating to Back-up and Recovery and retention of the system. Detail is covered in sub-requirements:</p> <ul style="list-style-type: none"> • NFR-MAS.5.3.1 – Compliance • NFR-MAS-5.3.2 – Failover 	

2.5.3.1 Compliance

BR ID:	NFR-MAS-5.3.1	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Compliance	
Requirement Description:	<p>A backup log must be maintained. The Customer expects backups to be on different physical storage as the data that is being backed up, they are automated, are tested by the Supplier</p> <p>The Customer prefers all our information including backups and all support to be in mainland UK. Any services offered in the EEA will be reviewed by the Customer's Security to determine if they are fit for purpose. Any services offered outside the EEA will be referred to Cabinet Office who will make a final decision as to their suitability.</p>	

2.5.3.2 Failover

BR ID:	NFR-MAS-5.3.2	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: S

Comments:	
Requirement Title:	Failover
Requirement Description:	Data loss must not occur as a result of the failure of any single component of the System.

2.5.4 Service Design

BR ID:	NFR-MAS-5.4	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Service Design		
Requirement Description:	The Service must support SaaS Principles and the Customer's need to be able to efficiently change Services in the future. It should provide loosely coupled interfaces between Service structures allowing flexibility for future change.		

2.5.5 System Lifecycle and Support

BR ID:	NFR-MAS-5.5	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	System Lifecycle and Support		
Requirement Description:			

Describes the non-functional requirements relating to the system lifecycle support. Detail is covered in sub-requirements:

- NFR-MAS-5.5.1 – ITIL
- NFR-MAS-5.5.2 – Incident Management
- NFR-MAS-5.5.3 – Upgrade / Patching
- NFR-MAS-5.5.4 – License Management
- NFR-MAS-5.5.5 – Working with the SIAM
- NFR-MAS-5.5.6 – Software Distribution
- NFR-MAS-5.5.7 – IT Service Continuity Management
- NFR-MAS-5.5.8 – Service Level Management
- NFR-MAS-5.5.9 – Problem Management
- NFR-MAS-5.5.10 – Root Cause Analysis
- NFR-MAS-5.5.11 – Service Improvement
- NFR-MAS-5.5.12 – Risk Management
- NFR-MAS-5.5.13 – Request Management
- NFR-MAS-5.5.14 – Service Desk
- NFR-MAS-5.5.15 – Capacity Management

2.5.5.2 ITIL

BR ID:	NFR-MAS-5.5.1	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	S
Status:	New		
Comments:			
Requirement Title:	ITIL		
Requirement Description:	The Supplier shall deliver all Services in alignment with best practice including the ITIL v3 IT Service Management (ITSM) lifecycle. The System must be designed in line with those practices.		

2.5.5.2 Incident Management

BR ID:	NFR-MAS-5.5.2	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Incident Management		
Requirement Description:			

Describes the requirements for fault detection and incident management. It covers the following sub-categories:

- NFR-MAS-5.5.2.1 – Fault Allocation
- NFR-MAS-5.5.2.2 – Fault Detection
- NFR-MAS-5.5.2.3 – Fault Resolution
- NFR-MAS-5.5.2.4 – Disruption to Service
- NFR-MAS-5.5.2.5 – Incident Single Point of Contact (SPOC)

2.5.5.2.1 Fault Allocation

BR ID:	NFR-MAS-5.5.2.1		
Functional Category:	Maintainability and Support (MAS)	Originator/Source:	
Status:	New	Priority:	M
Comments:			
Requirement Title:	Fault Allocation		
Requirement Description:			
The Supplier shall investigate and resolve incidents allocated to it in accordance with the Service Levels.			

2.5.5.2.2 Fault Detection

BR ID:	NFR-MAS-5.5.2.2		
Functional Category:	Maintainability and Support (MAS)	Originator/Source:	
Status:	New	Priority:	S
Comments:			
Requirement Title:	Fault Detection		
Requirement Description:			
The System must be designed so that faults can be easily detected and resolved. The Supplier shall:			
<ul style="list-style-type: none"> • assess the probable cause of a fault • notify the customer of the fault within the accepted SLAs • notify the Customer's Service Desk of the fault if appropriate and in agreement with procedures • instigate the Customer's Incident Management Process to provide information to its stakeholders if appropriate 			

2.5.5.2.3 Fault Resolution

BR ID:	NFR-MAS-5.5.2.3		
Functional Category:	Maintainability and Support (MAS)	Originator/Source:	
Status:	New	Priority:	M

Comments:	
Requirement Title:	Fault Resolution
Requirement Description:	
<p>Once the incident has been identified. The Supplier shall:</p> <ul style="list-style-type: none"> • repair the fault, as appropriate • carry out scripted function testing • restore the system to its appropriate configuration • test the system to ensure it is functioning correctly • notify the Customer of the fault resolution 	

2.5.5.2.4 Disruption to Service Resolution

BR ID:	NFR-MAS-5.5.2.4		
Functional Category:	Maintainability and Support (MAS)	Originator/Source:	
Status:	New	Priority:	M
Comments:			
Requirement Title:	Disruption to Service Resolution		
Requirement Description:			
<p>The Supplier must provide a plan for Disruption to Service incidents within one working day.</p> <p>See Glossary for definitions of Disruption to Service levels</p>			

2.5.5.2.5 Incident Single point of Contact

BR ID:	NFR-MAS-5.5.2.2.5		
Functional Category:	Maintainability and Support (MAS)	Originator/Source:	
Status:	New	Priority:	M
Comments:			
Requirement Title:	Incident Single Point of Contact		
Requirement Description:			
<p>The Supplier must assign and provide a Single Point of Contact in the event of a Disruption to Service or critical service level failure incident being raised, to support the incident process.</p>			

2.5.5.3 Upgrade / Patching

BR ID:	NFR-MAS-5.5.3		
Functional Category:	Maintainability and Support (MAS)	Originator/Source:	
Status:	New	Priority:	M
Comments:			
Requirement Title:	Upgrade / Patching		
Requirement Description:			

Any upgrades to the System or patches shall be fully tested to industry standards and best practice with documented evidence prior to implementation and should be applied seamlessly. If down time is required it should be agreed in advance with the Customer.

2.5.5.4 License Management

BR ID:	NFR-MAS-5.5.4	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	License Management		
Requirement Description:	Licenses should be utilised in the most cost effective manner available. Any additional licenses associated with the System must be managed by the Supplier on behalf of the Customer. Licenses must be transferable to new members of staff as appropriate.		

2.5.5.5 Working with the SMA

BR ID:	NFR-MAS-5.5.5	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	S
Status:	New		
Comments:			
Requirement Title:	Working with the SMA		
Requirement Description:	The Customer operates a 'Tower' model for its ICT services, with Service Management Assist (SMA) managing and overseeing problem solving and change implementation across the various Towers. The Supplier shall allow for such a SMA Tower model. The Service should align and support the Customer in the delivery of end to end service outcomes.		

2.5.5.6 Software Distribution

BR ID:	NFR-MAS-5.5.6	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Software distribution	
Requirement Description:		
<p>The System must be designed such that it requires the least amount of device specific configuration. There will be minimal distribution of software to the End User Device. If you do have to install something it should be installed via the HE Software Distribution tools.</p> <p>If there is a need to distribute software, then Supplier shall work with the Tower Supplier to ensure that:</p> <ul style="list-style-type: none"> • Software can be installed silently without requiring the end user to have administrative privileges (unless otherwise agreed with the Customer) • Existing Applications are unaffected when new applications are installed • Operating system or other Applications (both functional and non-functional characteristics) are not adversely affected when software is uninstalled • Upgrade Software is distributed when a new release is available as soon as is practical after the software distribution package passes the relevant testing. • Applications must be device and operating system agnostic <p>Where an application is to be utilised outside the Highways England IT estate, then the application shall:</p> <ul style="list-style-type: none"> • Follow industry standards for application development, deployment and maintenance • Be clear on the permissions required for its usage • Work on the major operating systems in usage by major mobile device manufacturers 		

2.5.5.7 IT Service Continuity Management

BR ID:	NFR-MAS-5.5.7	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	IT Service Continuity Management	
Requirement Description:		
<p>Describes the requirements for the management of Service Continuity. It includes:</p> <ul style="list-style-type: none"> • NFR-MAS-5.5.7.1 – Service Continuity Planning • NFR-MAS-5.5.7.2 – Service Continuity Testing • NFR-MAS-5.5.7.3 – Service Continuity Notification • NFR-MAS-5.5.7.4 – Service Continuity and the SMA 		

2.5.5.7.1 Service Continuity Planning

BR ID:	NFR-MAS-5.5.7.1	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	IT Service Continuity Planning		
Requirement Description:	<p>The Supplier should provide, update and share its Service Continuity plans for the resources and capabilities provided. These should include Impact Assessments and Risk Assessments appropriate to the service being provided. The Supplier shall manage Service Continuity risks for the system, including maintaining descriptions of possible and high probable crisis situations and incorporating mitigation and contingency actions into the ITSCM Plans (scenario planning)</p>		

2.5.5.7.2 Service Continuity Testing

BR ID:	NFR-MAS-5.5.7.2	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	S
Status:	New		
Comments:			
Requirement Title:	Service Continuity Testing		
Requirement Description:	<p>The Supplier should test its Service Continuity plans on a periodic basis and make available suitable evidence confirming the validity of the Service Continuity Plans and their appropriateness to achieve the Recovery Time Objective (RTO) as stated by the Supplier.</p>		

2.5.5.7.3 Service Continuity Notification

BR ID:	NFR-MAS-5.5.7.3	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Service Continuity Notification		
Requirement Description:	<p>The Supplier must notify the Customer in the event of instigating its Service Continuity Plan, where such action will have an impact on the service provided to the Customer's users.</p>		

2.5.5.7.4 Service Continuity and the SMA

BR ID:	NFR-MAS-5.5.7.4	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Service Continuity and the SMA		
Requirement Description:	<p>The Supplier must engage with the SMA (and any successor) and instigate and support incident management in the event of the instigating a Service Continuity Plan as a result of a failure of the Service. Notwithstanding that there is no requirement to notify SIAM prior to invoking Disaster Recovery protocol.</p>		

2.5.5.8 Service Level Management

BR ID:	NFR-MAS-5.5.8	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Service Level Management		
Requirement Description:			
<p>The Supplier shall provide and deliver the system to the agreed availability and design criteria and propose Service Levels, Service Level Targets and Key Performance Indicators for new or changed system components in a timely manner.</p> <p>In doing so the Supplier shall provide all relevant information relating to Service Levels, Service Level Targets and Key Performance Indicators for the system.</p> <p>It includes the following requirements:</p> <ul style="list-style-type: none"> • NFR-MAS-5.5.8.1 – Resolution (fix) Levels • NFR-MAS-5.5.8.2 – Service Forecasts • NFR-MAS-5.5.8.3 – Service Utilisation 			

2.5.5.8.1 Service Resolution Levels

BR ID:	NFR-MAS-5.5.8.1	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Service Resolution (fix) Levels		
Requirement Description:			
<p>The Service should provide support Target Resolution times to events/service requests</p> <p>For Information the Customer would consider the following resolution times as reasonable:</p> <ul style="list-style-type: none"> • Disruption to Service : Resolution (fix) time within 4 hours 			

2.5.5.8.2 Service Forecasts

BR ID:	NFR-MAS-5.5.8.2	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	S
Status:	New		
Comments:			
Requirement Title:	Service Forecasts		
Requirement Description:			
<p>The Supplier should provide reporting information as requested to ensure the Customer has visibility of any expected changes to Service Levels (outside the agreed SLAs).</p>			

2.5.5.8.3 Service Utilisation

BR ID:	NFR-MAS-5.5.8.3	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: C
Comments:		
Requirement Title:	Service Utilisation	
Requirement Description:		
<p>The Service should provide a mechanism for the Customer to be able to see the resources being utilised/consumed and the costs associated with those resources so that the Customer can easily determine the status of the Service.</p>		

2.5.5.9 Problem Management

BR ID:	NFR-MAS-5.5.9	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: C
Comments:		
Requirement Title:	Problem Management	
Requirement Description:		
<p>The Supplier shall provide a Problem Management Service that proactively seeks to prevent Incidents from happening within the system, and minimise the impact of Incidents that cannot be prevented.</p> <p>The Supplier shall analyse, monitor, progress, resolve and review Problems in line with the Service Levels.</p> <p>The Supplier shall provide Problem analysis and management information to the client including, but not limited to, information relating to Problem trends, volumes and Problem solutions. This shall be provided on a monthly basis in Word format.</p>		

2.5.5.10 Root Cause Analysis

BR ID:	NFR-MAS-5.5.10	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: S
Comments:		
Requirement Title:	Root Cause Analysis	
Requirement Description:		
<p>In the case where the Customer's end to end Service outcomes do not meet business requirements, the Supplier, when requested, must support the Customer in the Root Cause Analysis process, to support the investigation and subsequent resolution.</p>		

2.5.5.11 Service Improvement

BR ID:	NFR-MAS-5.5.11	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: S
Comments:		
Requirement Title:	Service Improvement	
Requirement Description:		
<p>The Supplier shall identify and notify to the Customer any process and system improvements and recommendations for consideration in respect of the services provided.</p>		

2.5.5.12 Risk Management

BR ID:	NFR-MAS-5.5.12	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: S
Comments:		
Requirement Title:	Risk Management	
Requirement Description:	<p>The Supplier shall identify and mitigate any emergent risk to the provision of the System.</p> <p>The Supplier shall implement any measure identified to address any emerging risk which has been approved by the Customer.</p>	

2.5.5.13 Request Management

BR ID:	NFR-MAS-5.5.13	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: C
Comments:		
Requirement Title:	Request Management	
Requirement Description:	<p>The Service must ensure the individual Service Requests assigned to them by authorised and agreed channels, are fulfilled within the service level target. Service Requests must be tracked and audited.</p>	

2.5.5.14 Service Desk

BR ID:	NFR-MAS-5.5.14	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Service Desk	
Requirement Description:	<p>Covers the requirements for the Supplier's Service Desk. Including:</p> <ul style="list-style-type: none"> NFR-MAS-5.5.14.1 – Service Desk Provision NFR-MAS-5.5.14.2 – Call Tracking 	

2.5.5.14.1 Service Desk Provision

BR ID:	NFR-MAS-5.5.14.1	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Service Desk Provision	
Requirement Description:	<p>The Service must provide a Service Desk, which will liaise with the Customer to ensure prompt resolution of requests or incidents in line with agreed Service Levels.</p>	

2.5.5.14.2 Call Tracking

BR ID:	NFR-MAS-5.5.14.2	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Call Tracking		
Requirement Description:	The Service Desk operation must track all calls from initial contact through to resolution. The Service must track the status of each open incident/request and manage its progression through to resolution/fulfilment.		

2.5.5.15 Capacity Management

BR ID:	NFR-MAS-5.5.15	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Capacity Management		
Requirement Description:	Describes the capacity requirements for the Service. It includes: <ul style="list-style-type: none"> NFR-MAS-5.5.15.1 – Elasticity of Service NFR-MAS-5.5.15.2 – Peak Demand 		

2.5.5.15.1 Elasticity of Service

BR ID:	NFR-MAS-5.5.15.1	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Elasticity of Service		
Requirement Description:	The Service must support the elastic provision of SaaS resources, supporting the requested increase and decreases of resources in line with demand, subject to appropriate demand controls.		

2.5.5.15.2 Peak Demand

BR ID:	NFR-MAS-5.5.15.2	Originator/Source:	
Functional Category:	Maintainability and Support (MAS)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Peak Demand		
Requirement Description:	The Service must support peak load user activity inside the levels of Service purchased.		

2.5.6 Data Centre

BR ID:	NFR-MAS-5.6	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: S
Comments:		
Requirement Title:	Data Centre	
Requirement Description:		
Cloud data storage should be used. Alternatively, HE are open to the supplier providing use and support of their own Data Centre.		

2.5.7 Data Centre Location

BR ID:	NFR-MAS-5.7	
Functional Category:	Maintainability and Support (MAS)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Data Centre Location	
Requirement Description:		
The Service should utilise Datacentres located in the UK, however Datacentres located in the EEA must be assured by independent validation of assertion.		

2.6 Security Requirements (SEC)

BR ID:	NFR-SEC-6.0	
Functional Category:	Security (SEC)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Security Requirements	
Requirement Description:		
Describes the information security requirements of the service.		
<ul style="list-style-type: none"> • NFR-SEC-6.1 Web Security • NFR-SEC-6.2 Cloud Infrastructure Security • NFR-SEC-6.3 Third Party Suppliers • NFR-SEC-6.4 Visibility of Data Sharing 		

2.6.1 Web Security

BR ID:	NFR-SEC-6.1	
Functional Category:	Security (SEC)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Web Security	
Requirement Description:		
<p>Appropriate and effective security controls shall be employed to mitigate common cyber-attacks included in OWASP top 10. The supplier shall evidence the proposed controls are effective in managing the identified cyber-attacks. The list currently includes:</p> <ul style="list-style-type: none"> • A1 Injection • A2 Broken Authentication and Session Management • A3 Cross-Site Scripting (XSS) • A4 Insecure Direct Object References • A5 Security Misconfiguration • A6 Sensitive Data Exposure • A7 Missing Function Level Access Control • A8 Cross-Site Request Forgery (CSRF) • A9 Using Components with Known Vulnerabilities • A10 Unvalidated Redirects and Forwards 		

2.6.2 Cloud Infrastructure Security

BR ID:	NFR-SEC-6.2	
Functional Category:	Security (SEC)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Cloud Infrastructure Security	
Requirement Description:		
<p>Appropriate and effective security controls shall be employed by the supplier in the delivery of the service. The Supplier shall adhere to recognised cloud security frameworks for example the National Cyber Security Centre's 14 cloud security principles. The supplier shall demonstrate compliance with the guidance published. The principles currently include:</p> <ul style="list-style-type: none"> • Data in transit protection • Asset protection and resilience • Separation between users • Governance framework • Operational security • Personnel security • Secure development • Supply chain security • Secure user management • Identity and authentication • External interface protection • Secure service administration • Audit information for users • Secure use of the service 		

2.6.3 Third Party Suppliers

BR ID:	NFR-SEC-6.3		
Functional Category:	Security (SEC)	Originator/Source:	
Status:	New	Priority:	M
Comments:			
Requirement Title:	Third Party Suppliers		
Requirement Description:	<p>The Supplier shall ensure that all security requirements of this contract are cascaded to all third party suppliers, delivery partners and subcontractors. The Supplier shall conduct regular and reasonable assurance activities of all third party suppliers, delivery partners and subcontractors to demonstrate continued compliance with the requirements of this Contract.</p>		

2.6.4 Visibility of Data Sharing

BR ID:	NFR-SEC-6.4		
Functional Category:	Security (SEC)	Originator/Source:	
Status:	New	Priority:	M
Comments:			
Requirement Title:	Visibility of Data Sharing		
Requirement Description:	<p>The Supplier shall provide details of how Customer information is shared with, or accessible by, third party suppliers and their supply chains.</p>		

2.7 Legal (LEG)

BR ID:	NFR-LEG-7.0		
Functional Category:	Legal (LEG)	Originator/Source:	
Status:	New	Priority:	M
Comments:			
Requirement Title:	Legal		
Requirement Description:	<p>The laws and standards which will govern the system. Sub-categories are:</p> <ul style="list-style-type: none"> NFR-LEG-7.1 Data Protection 		

2.7.1 Data Protection

BR ID:	NFR-LEG-7.1	Originator/Source:	
Functional Category:	Legal (LEG)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Data Protection		
Requirement Description:	<p>The System must comply with:</p> <ul style="list-style-type: none"> • General Data Protection Regulations (GDPR) and UK Data Protection Act 2018 reference: https://gdpr-info.eu/ and http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf • Freedom of information Act (FOI) 		

2.8 Service Transition (TRN)

BR ID:	NFR-TRN-8.0	Originator/Source:	
Functional Category:	Service Transition (TRN)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Service Transition		
Requirement Description:	<p>The requirements for successfully transitioning the service into operation. The sub-categories are:</p> <ul style="list-style-type: none"> • NFR-TRN-8.1 - Service Transition Planning • NFR-TRN-8.2 - Change and Evaluation • NFR-TRN-8.3 - Testing and Validation • NFR-TRN-8.4 - Configuration • NFR-TRN-8.5 - Knowledge Management • NFR-TRN-8.6 - Transition Support • NFR-TRN-8.7 - Data Portability 		

2.8.1 Service Transition Planning

BR ID:	NFR-TRN-8.1	Originator/Source:	
Functional Category:	Service Transition (TRN)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Service Transition Planning		
Requirement Description:	<p>The Supplier shall provide a plan of how the service shall be transitioned into operation including any risks associated with it. The plan shall include early life support provisions and shall be approved by the Customer.</p>		

BR ID:	NFR-TRN-8.2	
Functional Category:	Service Transition (TRN)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Change and Evaluation	
Requirement Description:	<p>Changes to the System must be scheduled, planned, assessed and implemented with authorisation of the Customer. The plan shall include, but not limited to:</p> <ul style="list-style-type: none"> • Undertake a Service Readiness Review to determine if HE is ready to adopt the change • Post Implementation Review • Acceptance Criteria • Back-Out Plans or Remediation Plans 	

2.8.3 Testing and Validation

BR ID:	NFR-TRN-8.3	
Functional Category:	Service Transition (TRN)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Testing and Validation	
Requirement Description:	<p>The System shall be tested as directed by the Customer including without limitation: Integration Testing; Operational Acceptance Testing; Regression Testing and User Acceptance Testing in participation with Service Readiness Reviews.</p> <p>The Supplier shall provide a test environment so that planned changes to the service can be tested by the Customer.</p>	

2.8.4 Configuration

BR ID:	NFR-TRN-8.4	
Functional Category:	Service Transition (TRN)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Configuration	
Requirement Description:	<p>The Supplier shall configure the System to the Customer's specification and provide the time it will take for the system set-up and Customer IT Infrastructure. The Supplier must provide full control and management of the Service's entire configuration, as expected as part of ISO20000, to ensure continuity, resilience and the ongoing meeting of service levels to the Customer. The Supplier must enable the Customer to configure basic elements of the System to be determined during transition.</p>	

2.8.5 Knowledge Management

BR ID:	NFR-TRN-8.5	
Functional Category:	Service Transition (TRN)	Originator/Source:
Status:	New	Priority: M
Comments:		
Requirement Title:	Knowledge Management	
Requirement Description:	<p>The Supplier must provide all documentation required in order for the Customer or any part of its Service structure to fully support the Customer users and business operations.</p>	

2.8.6 Transition support

BR ID:	NFR-TRN-8.6	Originator/Source:	
Functional Category:	Service Transition (TRN)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Transition Support		
Requirement Description:	The Service should include specialised support to facilitate transition to operation of new Services. This should include support for the Customer in managing the required business (e.g. organisational, roles) and technical (e.g. Service Management/SIAM interfaces) change needed to on-board those capabilities.		

2.8.7 Data Portability

BR ID:	NFR-TRN-8.7	Originator/Source:	
Functional Category:	Service Transition (SRN)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Data Portability		
Requirement Description:	The Service should enable the Customer to easily import and export Customer data through secured interfaces.		

2.9 Data Migration (MGR)

BR ID:	NFR-MGR-9.0	Originator/Source:	
Functional Category:	Data Migration (MGR)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Data Migration		
Requirement Description:	Describes the requirements covering the Data Migration activities. It is divided into the following sub-categories: <ul style="list-style-type: none">• NFR-MGR-9.1 – Data Migration Planning• NFR-MGR-9.2 – Data Migration Execution		

2.9.1 Data Migration Planning

BR ID:	NFR-MGR-9.1	Originator/Source:	
Functional Category:	Data Migration (MGR)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Data Migration Planning		
Requirement Description:	The Customer will require the Supplier to <u>support</u> in the on boarding of legacy data from Customer owned Systems. This will require the Supplier to take part in migration planning, activities and creating Data Migration Plans.		

2.9.2 Data Migration Execution

BR ID:	NFR-MGR-9.2		
Functional Category:	Data Migration (MGR)	Originator/Source:	
Status:	New	Priority:	M
Comments:			
Requirement Title:	Data Migration Execution		
Requirement Description:	<p>The Supplier will work with the Customer to undertake migration activity when required to support the transition of Customer owned data into the System. This will include but not limited to:</p> <ul style="list-style-type: none"> • Data Cleansing activities • Data Mapping activities • Data Archiving • Roll back provision • Data export and import 		

2.10 Exit (EXT)

BR ID:	NFR-EXT-10.0		
Functional Category:	Exit (EXT)	Originator/Source:	
Status:	New	Priority:	M
Comments:			
Requirement Title:	Exit		
Requirement Description:	<p>Describes provisions and duties and responsibilities of the Supplier leading up to and covering the expiry or termination of the Service in order to ensure a smooth and timely transition of the Services from the Supplier to a Replacement Supplier. It covers:</p> <ul style="list-style-type: none"> • NFR-EXT-10.1 – Exit Planning • NFR-EXT-10.2 – Exit Execution 		

2.10.1 Exit Planning

BR ID:	NFR-EXT-10.1		
Functional Category:	Exit (EXT)	Originator/Source:	
Status:	New	Priority:	M
Comments:			
Requirement Title:	Exit Planning		
Requirement Description:			

The Supplier shall within 60 working days from the start of the Contract deliver to the Customer an Exit Plan which sets out the Supplier's proposed methodology for achieving an orderly transition of Information and Services to the Customer and or a Replacement Supplier.

The Exit Plan shall cover as a minimum:

A detailed description of how the Assets and Services will be ceased and transferred including details of the processes, documentation, data transfer, systems migration, security and segregation of the Customer's technology components

- Details of inflight projects/incident/changes including current status and how they will be handed over
- Details of knowledge transfer proposals
- Proposals for training
- Documentation used in the provision of the Services and any Intellectual Property
- Proposals for the assignment or novation of all Services and support agreements utilised by the Supplier
- Proposals for the identification and return of all Assets
- Proposals for data migration
- Proposals for the disposal of any redundant Services and materials
- Details for the supply of any information or assistance required by the Customer or a Replacement Supplier

2.10.2 Exit Execution

BR ID:	NFR-EXT-10.2	Originator/Source:	
Functional Category:	Exit (EXT)	Priority:	M
Status:	New		
Comments:			
Requirement Title:	Exit Execution		
Requirement Description:			

During the termination period, set as the 90 calendar days preceding expiry or termination of the Contract, the Supplier shall comply with all the obligations contained in the Exit Plan.

The Supplier shall, on reasonable notice, provide any information related to the supply of the Services to the Customer or Replacement Supplier

The Supplier shall return to the Customer any of the following as appropriate:

- Copies of Customer owned Software and any other software licensed by the Customer to the Supplier under the contract
- All materials created by the Supplier under the contract, parts of the ICT Environment or any other equipment which belong to the Customer
- Any items which have been on-charged to the Customer such as consumables
- Each party shall return to the other party any confidential information
- Any licenses, leases or authorisations granted by the Customer to the Supplier in relation to the Services.

All data shall be preserved and made accessible for a set period of time, of at least 30 days, to allow data migration between services to be validated.

All records shall be exported into the Customer's EDRMS in agreed specified formats to agreed target areas, with all metadata including retention details.



online service network

SERVICE LEVEL AGREEMENT CONTINUITY OF SERVICE

Document Reference: 011/SLA/r2cTD/v4.0

This document and its content are copyright of r2c Online Limited © 2018. All rights reserved.

Any redistribution or reproduction of part or all of the contents in any form is prohibited. You may not, except with our express written permission, distribute or commercially exploit the content in any way. Nor may you transmit it or store it in any other way.

r2c Online Limited

A: 2 Vantage Drive, Sheffield, S9 1RG

T: +44 (0)114 399 2430 E: info@r2conline.com W: www.r2conline.com

Contents

Chapter	Contents	Page No.
1.0	Overview	3
2.0	Definitions	3
3.0	Limitations	4
4.0	Headline Service Level Deliverables	5
5.0	Service Level Deliverables	5
6.0	Scope of Service Provision	5
7.0	Change Requests	6
8.0	Issue Prioritisation	6
9.0	r2c Online Support Hierarchy	6
10.0	Support Engagement Procedure	7
11.0	Reporting	7
12.0	Escalation	7
13.0	Out-of-hours Support	8
14.0	Production Service Release Management Process	8
15.0	Hosting Provision	8
16.0	Network Infrastructure Management Process	8
17.0	Continuity of Operations/DR	10
18.0	Virus Protection	10
19.0	Environmental Software Maintenance	11
20.0	r2c Online Minimum System Requirements	12

Copyright Statement

Disclosure to Non-r2c Online Employees

This document may not be copied to, given to, copied by, or discussed with, any non-r2c Online employee, without first obtaining r2c Online's express permission in writing.

The information contained in this document is confidential and is submitted by r2c Online on the understanding that it will be used only by the recipient and staff or consultants to the recipient and that, where consultants are employed, their use of this information is restricted to use in relation to the business of the recipient. In particular, the contents of this document may not be disclosed, in whole or in part, to any other party without the prior written consent of r2c Online.

Copyright in this document remains vested in r2c Online Ltd. All rights reserved.

1.0 Overview

This document defines the Service Level Agreement between r2c Online and the Customer, and is applicable to the web based r2c Online Solution. We reserve the right, at our sole discretion, to update, change or replace any part of this service level agreement by providing 30 days notification via our website and platform. Your continued use of or access to our platform following the posting of any changes to this service level agreement constitutes acceptance of those changes.

2.0 Definitions

“Availability” - we will use commercially reasonable efforts to make the online Services available 24 hours a day, 7 days a week, except for: (i) planned downtime (of which we shall give advance notice), and (ii) any unavailability caused by circumstances beyond our reasonable control, including, for example, an act of God, act of government, flood, fire, earthquake, civil unrest, act of terror, strike or other labour problem (other than one involving our employees), Internet service provider failure or delay, Non-r2c Application, or denial of service attack.

“Business Continuity” means processes to be initiated to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

“Business Hours” means the hours between 09:00 and 17:30 GMT, excluding weekends and English public holidays.

“Change Request” means enhancements, modifications or additional functionality requirements that fall outside the Solution scope as defined in the standard release of r2c Online.

“Customer” means the company or organisation specified in the Order Schedule to which r2c Online is contracted to deliver the Solution.

“Disaster Recovery” means processes to be initiated to restore our system to a state of normality following significant negative events.

“Environmental Software” means any additional software required for operation of the Solution, inclusive of all Microsoft® and Third Party products and utilities.

“Hosting Partner” means r2c Online’s dedicated third party hosting provider.

“Installation Set” means a specific updated version of the Solution.

“ISP” means the Third Party organisation providing hosting services (Internet Service Provider).

“Issue” means a failure of the Solution to function in accordance with normal operating procedures (bug) as confirmed by r2c Online, not a request for new functional behaviour.

“Resolution” means the satisfactory remedy or response to an issue.

“Resolution Time” means the time elapsed from the point of response to the time that r2c Online submits a Resolution.

“Response Time” means the time elapsed from the receipt of notification of an issue to the time the r2c Online confirm receipt of notification of the issue.

“**RPO**” means recovery point objective – the point in time where data will be restored from.

“**RTO**” means recovery time objective – the target time to have the data restored.

“**Significant Negative Event**” means a sudden accident or a natural catastrophe that causes great damage or loss of life.

“**Solution**” means all or any part (according to context) of the Solution as delivered, including any services provided by r2c Online to the Customer in relation thereto.

“**Support**” means the services provided by r2c Online pursuant to this Service Level Agreement.

“**Workaround**” means a temporary repair or patch or replacement (whether or not such replacement is with a previously error-free version) of the Solution sufficient to allow the Solution to function albeit with limitations pending a Resolution.

3.0 Limitations

This SLA and any applicable Service Levels do not apply to any performance or availability issues:

Due to factors outside our reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure external to our data centres, including at your site or between your site and our data centre);

That result from the use of services, hardware, or software not provided by us, including, but not limited to, issues resulting from inadequate bandwidth or related to third-party software or services;

Caused by your use after we advised you to modify your use, if you did not modify your use as advised;

During or with respect to preview, pre-release, beta or trial versions of a feature or software (as determined by us);

That result from your unauthorised action or lack of action when required, or from your employees, agents, contractors, or vendors, or anyone gaining access to our network by means of your passwords or equipment, or otherwise resulting from your failure to follow appropriate security practices;

That result from your failure to adhere to any required minimum requirements specification, follow any policies for acceptable use, or your use in a manner inconsistent with the features and functionality of the software (for example, attempts to perform operations that are not supported) or inconsistent with our published guidance;

That result from faulty input, instructions, or arguments (for example, requests to access files that do not exist);

That result from your attempts to perform operations that exceed prescribed quotas or that resulted from our throttling of suspected abusive behaviour;

For licenses reserved, but not paid for, at the time of the Incident.

4.0 Headline Service Level Deliverables

1. Solution to be provided 24 hours a day 365 days a year
2. Solution to deliver 99.9+% availability. The Uptime Percentage is calculated over a rolling 12 month period using the following formula:

Uptime Percentage		
Total number of minutes in the last 12 months	MINUS	Total number of minutes of downtime in the last 12 months
Total number of minutes in the last 12 months		

3. Customer Support services available 9am – 17:30pm GMT Monday to Friday (excluding UK public holidays)
4. Planned downtime to be notified to the Customer in advance
5. Issues to be resolved within Resolution Times as defined within this document

5.0 Service Level Deliverables

r2c Online Commitment

r2c Online will ensure that any issue within with the scope of this SLA arising from the use of the Solution will be resolved, in a timescale which varies with reference to the severity of the issue, to the reasonable satisfaction of both the Customer and r2c Online. The commercial terms of this agreement are contained with our Standard T&C contained on our order form.

Customer Commitment

The Customer commits to:

1. Abide by the mechanisms for notifying r2c Online of an Issue with the Solution, as detailed within this document
2. Provide sufficient information to enable r2c Online to promptly identify and correct service issues
3. Provide a timely and meaningful response to legitimate r2c Online requests for further supporting information, re-testing, or clarification

6.0 Scope of Service Provision

Exclusions

This Service Level Agreement specifically excludes Customer end user support and provides a service level support framework for interaction with nominated Customer IT department/ project specific business contacts only.

r2c Online reserves the right to recover costs, against agreed time and material rates, any expenditure incurred by non-conformance of the Customer or their solution partners in this matter, and in the timely provision of agreed information and/or Support services.

7.0 Change Requests

Customer specific Change Requests can be logged via the helpdesk as per operational issues and they will be escalated to the appropriate commercial contact within r2c Online. These will be classified as roadmap items or a customer specific bespoke item for pricing and further Customer discussion.

Where Change Requests are implemented such that they introduce additional Customer-specific functionality, a fee equivalent to 20% of the agreed value of the Change Requests will be added to the platform usage fees on renewal to cover the additional Support burden.

8.0 Issues Prioritisation

The Response Time to an Issue varies depending on the severity of the Issue. The following table shows the definitions for the four priorities which can be assigned to a problem, and the Response Times for each priority level.

Priority Level	Description	Target Response Time	Target Resolution Time (From Time of Response)
1	System wide problems that prevent the utilisation / function of the solution as a whole and affect more than 5% of the users of the system.	1 hour	4 business hours
2	System wide problems that prevent utilisation/function of the solution which doesn't affect the system as a whole and/or affects less than 5% of the users of the system.	4 hours	48 business hours
3	Issues that do not impact core functionality of the system or only affect individual users.	4 hours	Will be prioritised and added into the next available development cycle
4	Minor or cosmetic problems with the solution, that do not affect functionality and do not stop users accessing and using the system.	4 hours	Will be prioritised and added into the next available development cycle

Response Times are measured from the time the Issue is recorded on the Helpdesk system, to the time at which r2c Online confirms receipt of the issue notification. Resolution Times are measured from the time the issue is confirmed to the time r2c submits the resolution to the Client for approval. Where recorded Issues require any Client action or response, the time taken for such action (i.e. when issue ownership is outside r2c Online boundaries) will not be counted against Resolution Time.

All Response and Resolution Times are related to business hours - i.e. if a priority 4 Issue is logged at 16.30pm, our Service Team have until 12pm lunchtime the next working day.

9.0 r2c Online Support Hierarchy

First Line Support – The r2c Online Support Team and Helpdesk provides initial point of contact to all stakeholders and co-ordinates internal Resolution and stakeholder notification(s).

Second Line Support – The r2c Online Technical/Development Team provides Resolution of service queries requiring more detailed technical expertise and analysis.

10.0 Support Engagement Procedure

The Customer will nominate named service contacts for filtering and channelling end user issues into the r2c Online Helpdesk. Telephone or email submission is the preferred communication option with each request being recorded on our internal support system.

Support Process

If nominated Customer Solution contacts have any technical problems or queries with the Solution, the following procedure should be followed:

1. E-mail r2c Online at designated address or phone the Helpdesk facility to submit an Issue
2. The Helpdesk application will record the details of the Issue, prioritise the Issue against agreed prioritisation levels and confirm to the stakeholder accordingly
3. The priority level ascribed will be at the discretion of r2c Online, acting reasonably and in the best interests of resolving the Issue on a timely basis to the mutual satisfaction of the Customer and r2c Online
4. The Issue will be entered into a secure Customer environment within the r2c Online Helpdesk application
5. All Issues will be allocated a service level request number. This number will be used to track the progress of the service Issue and its Resolution. The Customer Support Team allocates suitable resource to satisfy service request Resolution within defined timescales and maintains control of internal ownership and workflow processes
6. r2c Online will enact Resolution in compliance with any agreed and documented processes for internal issue management and release management processes
7. Any Issues deemed by r2c Online to constitute a Change Request will trigger formal pricing/delivery proposal mechanisms, external to the SLA procedure

When the service request is resolved, r2c Online will inform the Customer by phone or via email. This will detail the Resolution of the service request and the time it was resolved. Should there be a disagreement as to the effective Resolution of the service request; the Issue will be returned to an active status for further investigation.

Where it is necessary to reopen a service level request, the SLA will continue from the point at which it was stopped, rather than starting over again.

11.0 Reporting

r2c will provide reporting on performance against this SLA measured on a monthly basis. The provision and delivery of reporting will be agreed between the Customer and the r2c account manager.

12.0 Escalations

If at any time the Customer is unhappy with any aspect of support service delivery, a request should be entered to the Customer Support Team to escalate the matter to the r2c Online Operations Manager. r2c Online will work with the nominated Customer contact to achieve a mutually agreeable Resolution.

13.0 Out-Of-Hours Support

Outside of normal business hours, problems should be logged by email or via voicemail, where they will be queued for Resolution the following business day. Standard quoted Response Times apply from commencement of Business Hours as defined in this document.

14.0 Production Service Release Management Process

No service application changes will be released to the production environment without notification to the Customer. As this is a platform there will be regular maintenance updates every quarter and as required, patches that will be applied out of hours normally on a Sunday. As stated above, the Customer will be notified of planned maintenance at least 14 days in advance, where possible.

15.0 Hosting Provision

The hosting service provided by r2c Online on behalf of the Customer is a fully managed service inclusive of all hardware, software, network infrastructure, security, disaster recovery and bandwidth provision.

The Customer Solution is hosted external to r2c Online through a contracted Hosting Partner. At the time of this contract the service provider is based in the United Kingdom at two private, secure data centres.

r2c Online may vary its Hosting Partner after giving the Customer at least one month's written notice and on condition that any such change will not have a detrimental effect on the contract or any other service level agreed between r2c Online and the Customer.

16.0 Networking Infrastructure Management Services

System Performance and Scalability

r2c Online will ensure that the infrastructure under its control, or under the control of its chosen Hosting Partner, will operate within workload criteria appropriate to the performance of the Customer Solution.

r2c Online will commit to monitoring all components on a continuous basis to ensure they operate within an acceptable range. Where a workload exceeds any acceptable threshold, r2c Online will, in conjunction with its Hosting Partner, instigate a follow-up to address any underlying issues at no cost to the Customer.

System Monitoring and Scalability

r2c Online business systems are pro-actively monitored on a 24-hour, 7-day basis to ensure achievement of availability and performance targets referred to within this document. Availability monitoring is provided at a number of different levels from front-end application availability through to infrastructure component availability.

We are monitoring over 800 items including but not limited to, the following:

- Availability
- Data load times
- SQL performance
- Network cards
- Memory availability
- Pagefile size
- CPU/Processor Load
- Load balancing

r2c Online employs a strict change management approach for all changes to the production environments. This is operated in conjunction with r2c Online's Hosting Partner. All changes to any element of the production environment are logged and details of these are retained for inspection if required.

All changes are tested and verified as being appropriate to production standards in advance of implementation.

r2c Online systems will be available in accordance with the following timelines:

1. r2c Online in conjunction with its Hosting Partner, will use all commercially reasonable efforts to achieve 99.9+% availability of the elements within its control
2. 24 hours per day x 7 days per week x 365 days per year hardware monitoring, repair and support
3. 24 hours per day x 7 days per week x 365 days per year Internet access availability monitoring
4. Unlimited server traffic access
5. Planned service outages (hardware and software) for maintenance reasons will be restricted to agreed out-of-hours time periods where possible, unless with prior agreement from the Customer where possible

System Maintenance

In order to ensure the efficient running of its production environment, r2c Online reserves the right to use a scheduled maintenance period (as noted below) for the purpose of application upgrades and general system maintenance. Any intention to employ these maintenance windows will be notified to the Customer in advance.

1. A scheduled maintenance window may be employed for standard system infrastructure and application upgrades
2. Wherever possible, r2c Online will notify the Customer prior to the event

r2c Online also reserves the right to employ an emergency maintenance window for applying critical fixes to the production environment. All commercially reasonable endeavors will be made to inform the Customer before any outages and to limit the frequency and extent of these outages. r2c Online will make all reasonable efforts to schedule these outages at a time that will have minimal impact on the Customer.

1. If emergency maintenance is required it will take place, wherever possible, outside high demand hours
2. r2c Online will present a screen notifying the user where possible, but the very nature of an emergency outage means it is not feasible to present an expected time of return

17.0 Continuity of Operations/DR

System Access/Disaster Recovery

To facilitate recovery from hardware/environmental failure or access to site problems, r2c Online undertakes the following: -

1. A back-up is taken every 15 minutes of the system as it stands to an external DR site
This is on a separate infra-structure hosted externally to the main server
2. Back-up files are transferred to a back-up server every 15 mins, one week's worth of data is stored
3. We have a full data centre on standby more than 30 miles from the main site for use in the event of a major disaster on the main site
4. A further back-up is taken every 24 hours to a cloud-based platform
5. A new Installation Set will be generated whenever substantive changes are made to either the Customer Solution set or the associated environmental software. A back-up copy will be made and lodged off site
6. RPO (Recovery Point Objective) is 15 minutes
7. RTO (Recovery Time Objective) is 8 business hours

Business Continuity

To facilitate continued delivery of service in the event of disruptive incidents, r2c Online undertakes the following: -

1. We have committed to improving our Vantage Drive site to include a back-up power supply by means of an emergency automatically triggered generator to ensure ongoing service delivery in the event of failure
2. We have also committed to the installation of a second, independent fibre optic connection. This will approach the site from an alternative source and direction
3. Our site is monitored by over 200 sensors that instantly advise if hardware is failing to prompt preventative action
4. In the event that the site cannot be occupied, all of our staff are mobile and can operate through cloud-based management tools in any location including their home address if for a prolonged period of time
5. In addition to our Disaster Recovery back up process, our products are protected by over 500 system sensors that advise of any interruptions in system availability or functionality issues
6. We maintain and have instant access to 3 portal versions of our products and in the event of system issues we can instantly move users from one portal to the next with minimal interruption in service delivery

18.0 Virus Protection

r2c Online utilises antivirus software for protection against viruses on personal workstations and servers. In addition, r2c Online subscribes to all major virus warning email servers.

19.0 Environmental Software Maintenance

Microsoft supplies all critical environmental software used by r2c Online.

Microsoft has implemented a policy of releasing service packs and critical updates on a regular basis and r2c Online has a number of servers configured to automatically receive critical upgrades and is on the distribution list to receive notification of such upgrades.

As a Microsoft Gold Partner we always review and thoroughly test service packs prior to implementing the changes as part of the normal maintenance process.

In the case of critical upgrades, the policy is to install all such upgrades unless they do not have any benefit to be installed on the r2c Online Solution set.

Implementation Policy

r2c Online undertakes to implement all relevant virus protection updates as soon as is practical and consistent with maintaining a reliable and secure service to the Customer.

r2c Online undertakes to implement all service pack updates outside of the Customer specified support hours.

r2c Online undertakes to implement all critical upgrades as soon as is practical and consistent with maintaining a reliable and secure service to the Customer. r2c Online undertakes that where such an upgrade directly affects the critical day-to-day operation of the Solution then r2c Online will discuss such upgrades directly with the Customer in order to determine and agree an implementation policy.

Security

Key aspects of physical security measures are outlined below.

Technical Resilience

The Data Centre is protected as follows:

1. Under floor cooling systems
2. Dual power feed from disparate Customer stations
3. Twin UPS
4. Twin diesel generators (24-hour duty cycle)
5. 24-hour network monitoring
6. Argonite fire suppression

Network Infrastructure

The Data Centre is fully protected by Cisco ASA Firewall technology.

Physical Security

The Data Centre is protected by:

1. Non-branded building
2. Multiple alarms with direct police connection
3. Dual skinned walls and roof
4. Anti-Ram barriers
5. Motion and Vibration sensors throughout the facility
6. Nightly Estate Lock down with 24-hour monitoring by camera and security personnel
7. Reflective windows covered by metal shutters in hours of darkness
8. Internal 24-hour video surveillance
9. Swipe card access

20.0 r2c Online Minimum System Requirements



To use r2c Online or Offline on a tablet or PC:

Please note the following hardware, software and communications requirements are provided as an outline of what is required as a minimum to use the r2c Online solution effectively.

Portal (Administration Portal)

Hardware Requirements:

1. CPU: Pentium III or higher/400 MHz (recommended: 800 MHz or higher)
2. Main memory: 512 MB RAM (2GB recommended)
3. Wi-Fi enabled / wired connection point for internet access.
4. If using a Portal on a Tablet device (Windows or Android) then a minimum screen size of 10" is required.

Software Requirements:

1. Operating System:
 - Windows 8 and above
 - Android 6 and above
 - iOS9 and above
2. Adobe Acrobat Reader v9.0: is used to open PDF inspections (version 9 or above recommended)
3. Cookies must be activated

Inspect (Technician Side)

Hardware Requirements:

1. CPU: Pentium III or higher/400 MHz (recommended: 800 MHz or higher)
2. Main memory: 512 MB RAM (2GB recommended)
3. Wi-Fi enabled / wired connection point for internet access.
4. If using Inspect on a Tablet device (Windows or Android) then a minimum screen size of 10" is required.
5. Touch Screen: This is a requirement for r2c Inspect if you wish to use as a touch screen. (Note: however that all of r2c can be used on a PC with a mouse and keyboard)
6. Given the normal working environments, a ruggedized and durable piece of hardware is recommended.

Software Requirements:

1. Browser plug-in: Adobe Acrobat Reader v8.0 (or above recommended)
2. Adobe Acrobat Reader v9.0: is used to open PDF inspections (version 9 or above recommended)
3. Operating System:
 - Windows 8 and above
 - Android 6 and above
 - iOS 9 and above

Screen Resolutions:

1. 1024 x 768 pixels or higher with a minimum of 256 colours
2. 1366 x 768
3. 1280 x 1024
4. If using either Portal or Inspect on a Tablet device (Windows or Android) then a minimum screen size of 10" is required.

Browsers:

1. Internet Explorer 10 and above
2. Mozilla FireFox (any version as this automatically updates)
3. Google Chrome (any version as this automatically updates)

Driver Pre-Use Check Software

Web Version:

1. Browser required as above

iOS:

1. Version – iOS version 9 and above
2. Screen size – iPod Touch / iPhone 4 upwards

Android:

1. Version – 6 or higher
2. Memory – minimum 512mb
3. Screen resolution – minimum resolution 800 x 480, recommended 1200 x 720 or higher

iService Desk

1. Browser – Internet Explorer 10 and above with Microsoft Silverlight installed

Core platform

Service Specification



online service network

OVERVIEW

r2c Online's independent online platform has transformed the entire end-to-end management of compliance, maintenance, authorisation and invoicing for vehicles and associated assets.

Here you can find out about all the great features on r2c Online's core platform for your type of business.



DASHBOARD

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
Fleet Availability Optimise utilisation of your assets or workshops. r2c Online allows fleets to quickly see your asset availability and measure it against set benchmarks, alerting you to potential issues. For workshops, r2c allows you to monitor time to repair, tracking your performance against set benchmarks and alerting you to potential issues, maximising workshop throughput and minimising vehicle downtime.	✓	✓	✓
Compliance Breaches See your compliance status at a glance r2c Online features an overview dashboard, presenting a summary of key compliance, service and maintenance information at a glance. This allows management by exception, with the platform flagging those events or issues that require management intervention, helping you manage downtime in real-time, driving efficiency.	✓	✓	✓
MOT Pass Rates Understand your First Time pass rate MOT results can be recorded directly into the system giving you powerful, real time, data on your First Time Pass Rates, reasons for failure and even measuring your performance against the whole r2c network.	✓	✓	✓
Outstanding Defects Defect reporting and management r2c's electronic workflow for the workshop manages defects by exception, ensuring faults or service requirements are brought to the attention of the foreman or supervisor for review. Authorisation can then be sought from the client where necessary, allowing the work to be completed without delay.	✓	✓	✓

Job Tracking

Live track your vehicle downtime

Minimising downtime, means having real time data shared between parties. r2c Online seamlessly connects all relevant parties, both internal and external, so job status's can be tracked without the need for phone calls and emails.



Booking Requests (requires i2i Bolt On Product)

Electronic Booking requests take the guesswork out of achieving the optimal service arrangements

Fleet management and operators can make booking requests electronically which are instantly relayed to the relevant service provider. These are then checked and confirmed online, updating the service plan automatically and giving both parties an accurate and comprehensive picture of the planned maintenance and repair for each vehicle, asset and ancillary. In the event that a requested slot is not available, the service provider can suggest alternatives for the fleet operator to check and authorise.



Authorisation Requests (requires i2i Bolt On product)

Simple Electronic Authorisation - for fleet management and operators

For fleets and vehicle operators, the r2c platform delivers a range of e-commerce based services that simplify and reduce the cost of managing work authorisations and inspections. Before

using r2c Online, many fleets described the unwieldy game of 'table tennis' they used to play with vehicle dealers and workshops, with numerous phone calls, emails and faxes going back and forth to authorise and pay for even the most basic of repairs.

Simple Electronic Authorisation - for dealers and workshops

Switching to paperless, electronic quoting and authorisation dramatically cuts the cost of dealing with every transaction, saving time, streamlining resource required and ensures timely and accurate invoicing every time. Your fleet customers will notice the difference when they receive inspection reports and respond to quotes instantly, based on their agreed menu pricing. By authorising work straight away, it avoids any unnecessary downtime in the workshop and ensures asset utilisation is maximised for the customer. Plus you'll see a dramatic reduction in invoices being queried and a more efficient process to gain authorisation for work.



Driver Pre Use Checks (requires Driver Bolt On product)

Digitally capture pre use checks on any device & seamlessly manage defects to completion



<p>r2c Online automates and simplifies the process of driver pre-use checks. Drivers complete the checks on a mobile phone or mobile device as part of their pre use routine. The information is routed automatically and alerts the relevant person if defects have been found. The defect is then processed through the r2c defect management system, either by being immediately placed as a booking request for repair or allocated onto the next scheduled job. All defects recorded are safely and securely stored, linked to the relevant asset and the driver who did the check. This means an end to the problems of managing and capturing the data from manual checks.</p>	✓	✓	✓
<p>Time to Repair Standard repair time database</p> <p>With r2c Online, comprehensive standard and agreed repair times can be managed, whether the source of data is from the manufacturer, customer's own or industry standards such as ICME.</p>	✓	✓	✓



PLANNER
 Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
<p>Asset Schedule</p> <p>A complete maintenance plan for your whole fleet which allows you to share, collaborate and manage events in real time.</p> <p>With r2c, fleet managers, vehicle operators and dealers/workshops communicate and schedule Quote, Authorise & Invoices seamlessly, painlessly and dynamically. This is done via an automated collaborative scheduling system which creates a calendar of inspections and service visits for each and every asset. In addition, automatic reminders ensure that inspections are not missed, protecting your license to operate and ensuring the residual value of each and every asset/vehicle is maintained.</p>	✓	✓	✓
<p>Maintenance Planner</p> <p>Live Maintenance Plan and Wall Chart</p> <p>The live maintenance plan provides an up-to-the-minute forward schedule of all planned service, maintenance, repair and compliance activities for each asset or vehicle. The plan ties each event to the relevant associated paperwork, and only allows events to be closed down if the relevant paperwork is received.</p> <p>In addition, the plan is live and is shared dynamically between all interested parties, meaning amends or updates are visible to all. Events can be forward planned for up to 10 years, and</p>	✓	✓	✓

<p>once an asset or vehicle is scheduled at the start of the plan, it doesn't need to be periodically redone.</p> <p>Reporting is quick and simple, and can be segmented by different criteria. For instance events can be viewed by year, by customer or by depot or fleet. Finally, the schedule can be printed off at any point, can be emailed and can be used as a wall-planner.</p>	✓	✓	✓
<p>Schedule breaches</p> <p>Turn the lights back on and predict potential breaches</p> <p>And instantly see where potential compliance breaches are about to happen, alerting you as to when and where you need to take action to ensure 100% compliance.</p>	✓	✓	✓
<p>Configurable alerts</p> <p>Inspection/service due, overdue or missed</p> <p>Proactive alerts remind both the workshop and fleet operators that inspections are due. This prevents essential inspections and services being missed, avoiding the risk of non-compliance. In addition, reminder and overdue alerts help prevent no shows, protecting revenues for the workshop and ensuring missed events do not just slip through the net unnoticed and cause issues with compliance and higher overall maintenance costs.</p>	✓	✓	✓



ORGANISATION

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
<p>User Management</p> <p>Manage your users & Customise the look and feel of the application.</p> <p>Specify and control who can access what in r2c and change the colour scheme to match your brand more closely, uploading your corporate logo.</p>	✓	✓	✓
<p>Instant Messaging</p> <p>Never feel in the dark again with configurable messaging/alerting</p> <p>Choose who, when and how you want to be communicated to and about what events, customising an alerting system to your company's and individual's needs.</p>	✓	✓	✓

<p>Working Times</p> <p>Manage the operating hours of your organisation</p> <p>To enable full transparency with your customer and repairer base, r2c allows each organisation to record standard, weekend and out-of-hour operating times and even allocate labour rate multipliers to assist in i2i transactions.</p>			
<p>Tyre Type Management</p> <p>Manage multi-level tyre matrices to ensure your wheels keep rolling</p> <p>Select the brand and type of tyre your repairer network should supply, as well as custom tyre values including the minimum tyre depth and retorque requirements.</p>			
<p>Organisational Structure</p> <p>Build your company's hierarchy and align your fleet and users view accordingly</p> <p>No one company is ever structured the same and with r2c you can cut and slice your company into vertical and horizontal hierarchies, reflecting your depot network, your Operator Licences and your fleets, segmenting your users view to the elements they are interested in and customising reporting in line with your structure.</p>			
<p>User Groups (requires i2i bolt on product)</p> <p>Control authorisation limits within your organisation</p> <p>To assist with cost control i2i subscribers have the ability for authorisation limits to be set for each user within your organisation. This can vary by customer so multi-level groups have been provided.</p>			
<p>Services Provided</p> <p>Showcase your organisation by listing out services provided and your facilities to potential customers</p> <p>By keeping your organisation details up to date and defining what types of assets you work on, facilities you offer and what services you provide you can showcase your business in the r2c directory to customers and prospective customers alike.</p>			

Invoice Management (requires i2i Bolt On product)

E-Invoicing

Invoices are generated automatically, as a result of pre-authorisation of work. Electronic invoicing is quick and information flows instantly and seamlessly and can be automatically fed into customers accounting systems. This means a dramatic improvement in the efficiency of accounts payable, as well as cashflow management for the repairer, without having to wait for paper invoices to travel in the mail and be checked and validated. Any queries are dealt with during the authorisation process so that invoice queries become a thing of the past.



ASSETS

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
<p>Asset Details</p> <p>Know everything that you need to know about your assets instantly</p> <p>The online service file is a detailed record of each vehicle and asset, along with details of associated ancillary assets. It contains detailed records about the asset and captures a detailed audit trail of its life (including inspections, services and repairs). It allows you to build up a detailed picture of each and every asset or vehicle in your fleet.</p>			
<p>Vehicle off Road Log</p> <p>Having instant access to your vehicle status allows you to effectively manage downtime and increases your profits.</p> <p>With r2c Online you can instantly know which vehicles are off the road and why, tracking the reasons why and managing the actions in order to minimise the amount of downtime.</p>			
<p>Schedule Management</p> <p>Never miss an event again with automated and collaborative scheduling.</p> <p>With r2c, fleet managers, vehicle operators and dealers/workshops communicate and schedule Quote, Authorise & Invoices seamlessly, painlessly and dynamically. This is done via an automated collaborative scheduling system which creates a calendar of inspections and service visits for each and every asset. In addition, automatic reminders ensure that inspections are not missed, protecting your license to operate and ensuring the residual value of each and every asset/vehicle is maintained.</p>			

<p>Defect Management</p> <p>Seamlessly manage defects through to completion, tracking every step.</p> <p>The online service file captures detailed information about defects that are reported each time the vehicle or asset has an inspection (such as a statutory scheduled inspection or an MOT). Once defects are logged, the platform flags these defects, managing the process of repair. This ensures that defects are brought to management attention, minimising VOR (vehicle off road) time.</p>			
<p>Recall Management</p> <p>Ensure that Asset Recalls & Campaigns are efficiently communicated and resolved quickly with complete visibility of the process</p> <p>r2c Online brings together vehicle manufacturers, dealers, workshops, fleet management and operators together on a single platform. In the event of a manufacturer issuing a recall, this information can be relayed to both the repairing dealers and also affected customers immediately, allowing repairs or corrective action to be taken swiftly and effectively. This is in contrast to managing recalls through letters, which may not</p>			
<p>Document/Service History</p> <p>A complete, digital, Maintenance History, available anywhere, anytime</p> <p>The online service file captures a detailed record of all service, maintenance, repair and compliance events and allows operators, workshops and fleet management to access and update this information in real-time. This protects asset residual values, since you can prove that the correct maintenance and service intervals have been followed. Additional information, such as certificates and manuals, can be scanned onto the asset file to give a complete history.</p>			
<p>Maintenance History (requires i2i Bolt On)</p> <p>Real-time, tamper proof service history</p> <p>With r2c Online, your online service histories are updated instantly in real-time, so you always have an up-to-the-minute view. This ensures that your records always reflect the most recent activities such as inspections and repairs. The data is also safely secured in a 'digital vault', unlike paper copies which could be tampered with, lost or misplaced.</p>			

Contract Management

Transact business faster and cut your risk with electronic contract management.

The r2c Online solution streamlines the effective management of supplier and customer terms online, taking into account labour rates, repair times, parts prices, discounts, fluids and consumables. Once authorisation limits and contract types have been configured, the r2c platform will process transactions automatically within agreed limits. This avoids the need for manual review of each and every service, repair or inspection, whilst ensuring that costs and work carried out is in line with contract rules and budgets. Where necessary, items of work that fall outside the normal approval time, cost and resource parameters will be flagged for review and authorisation. Automated contract management reduces the unnecessary delays of waiting for approvals, allowing work to



JOB SHEETS

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
<p>Live KPI Tiles</p> <p>Instant access to visually rich KPIs displayed in tiles for instant reporting and interaction</p> <p>Have you ever wondered how you can instantly find out how many of your assets are in the workshop or due to go in today? Maybe you want to know which assets have documents outstanding, are currently under repair or are complete and ready to go back on the road. All this information and more is available at the press of a button so you can keep on top of any downtime.</p>			
<p>Job List</p> <p>Quickly view your jobs and what you need to work on.</p> <p>Our Jobsheet KPI filters provide key information that at a glance gives you a quick health check of outstanding work. Other more advance filters have been provided to enable you to drill down into the Jobsheet list.</p>			
<p>Digital Job sheets</p> <p>Always accessible job sheet/document storage, available for immediate viewing or download</p> <p>No more waiting on a grubby Jobsheets from your technicians, when the asset is in the workshop or in the field. Instantly view a completed Jobsheet that will be signed electronically by the technician and workshop supervisor.</p>			

Digital workflows

Workflows made simple

With r2c Online there's no more lost service sheets or grease-covered sheets of paper. Your engineers simply follow clear, simple and intuitive screens that guide them through every step and check in the service process. Nothing gets missed, there's no paperwork involved and engineers actually enjoy working with it. So everyone is happy. The information is relayed instantly to service reception, allowing them to send an update to the customer and a copy of the electronic service sheet instantly, without the need for administrative effort validating and auditing content for basic anomalies.



Electronic T Card Management

Ergonomic Job management to replicate legacy workshop T Card systems.

Sometimes the old ways are the best, particularly when you can do it digitally and in real time. Take the tried and tested T Card management system and provide a simple, graphical user interface to allow you to see the status of jobs at any time and from anywhere.





DOCUMENTS & SERVICE HISTORY

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
<p>Document History</p> <p>Detailed, robust and transparent audit trail.</p> <p>Unlike manual paperwork that can be lost, misfiled, misplaced or inadvertently destroyed, r2c Online provides a safe, secure and transparent record of all documentation and provides a robust audit trail of all activities and transactions. Key information can be instantly accessed on demand.</p> <p>Real-time, tamper proof service history.</p> <p>With r2c Online, your online service histories are updated instantly in real-time, so you always have an up-to-the-minute view. This ensures that your records always reflect the most recent activities such as inspections and repairs. The data is also safely secured in a 'digital vault', unlike paper copies which could be tampered with, lost or misplaced.</p>			
<p>Scanned documents</p> <p>Complete your document history by uploading any non-digital documents into your file.</p> <p>We know you need a comprehensive document history and there's some things you need to scan, upload and index. Maybe it's an MOT document, a Loler Certificate or maybe a service manual. Whatever it is you can do this direct to the asset history file or on a job sheet.</p>			
<p>Compliance breaches</p> <p>Digital document management allows you to instantly see any potential compliance breaches.</p> <p>By using r2c's document management system you can manage any compliance breaches, quickly and easily identifying any missing or incomplete documents so you can be sure you're on top of your compliance 24/7.</p>			



NETWORK MANAGEMENT

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
Supplier Networks Build and manage your trusted supplier networks through an Invitation only function. r2c Online is a secure private platform, giving you the power to grant access to only your chosen, trusted and preferred suppliers. This invitation-only system ensures your data is totally secure and private. You can also choose what level of visibility service providers have around your assets, vehicles and ancillaries.			
Supplier preferencing Create and maintain a hierarchy of suppliers aligned with KPIs and improve work penetration rates for best in class performers. Take the guess work out of which of your preferred suppliers you should send work to by grading them. Choose the right supplier based on a number of factors including services provided, opening times and distance / driving times.			
Customer Networks Multi network compatibility to broaden availability. Sometimes your own approved networks just aren't enough and they need to be augmented by a customers. You can do this simply with multi-network compatibility ensuring the right suppliers are chosen based on customer requirements and optimal allocation criteria.			
Supplier Directory Highly accurate supplier search tool matched to criteria input. Find new suppliers quickly and easily by using the extensive search facilities including by location, services provided, opening times, sectors, specialisms, franchise and more.			



REPORTING

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
<p>Reporting</p> <p>Instant on demand reporting suite.</p> <p>Comprehensive suite of more than 50 standard reports which can easily be segmented and downloaded as pdf, excel or csv files.</p>	✓	✓	✓
<p>Scheduled Reports</p> <p>Get the information you want, when you want it.</p> <p>Want a specific report sent to certain people at certain times, then our report scheduling functionality allows you to get the information you want, when you want it.</p>	✓	✓	✓



ALERTING & MESSAGING

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
<p>Configurable alerts</p> <p>Customise when, who and on what event/issue you want to be notified.</p> <p>Proactive alerts remind both the workshop and fleet operators that inspections are due. This prevents essential inspections and services being missed, avoiding the risk of non-compliance. In addition, reminder and overdue alerts help prevent no shows, protecting revenues for the workshop and ensuring missed events do not just slip through the net unnoticed and cause issues with compliance and higher overall maintenance costs.</p>	✓	✓	✓
<p>Real time communications</p> <p>Timed E-Booking requests, authorisation requests and Jobsheet updates.</p> <p>Organisational and user specific messages ranging from booking and Jobsheet updates, to i2i authorisations providing links to the important actions that are required. These messages are timed and provide all the key information you will require to manage your work flowscheduling functionality allows you to get the information you want, when you want it. Jobsheet updates, to i2i authorisations providing links to the important actions that are required. These messages are timed and provide all the key information you will require to manage your work flow.</p>	✓	✓	✓



ELECTRONIC BOOKINGS

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
<p>E-Bookings</p> <p>Phone calls, on hold messages, faxes, emails all become a thing of the past with instant E Bookings.</p> <p>Fleet management and operators can make booking requests electronically which are instantly relayed to the relevant service provider. These are then checked and confirmed online, updating the service plan automatically and giving both parties an accurate and comprehensive picture of the planned maintenance and repair for each vehicle, asset and ancillary. In the event that a requested slot is not available, the service provider can suggest alternatives for the fleet operator to check and authorise.</p>			
<p>Work required</p> <p>MOT, inspection and menu priced repairs can be requested electronically with additional defect reporting features available directly in the module</p> <p>A selection of commonly used work types available for selection including a guided vehicle specific tyre option. The defects raised within the module can be graded for severity and allow for defect numbers to be added to be recorded in the Defect Management module.</p>			
<p>Special Instructions</p> <p>We understand not all bookings are the same.</p> <p>The requirements stage allows a user to ensure the booking without the need for a phone call.</p> <p>Looking for an on-site repair, or a Courtesy vehicle? This can be requested along with the option to suggest multiple appointments in a single E-Booking, Change your mind? The E-Booking can be edited and even sent to an alternative repair agent.</p>			
<p>Supplier selection</p> <p>Search for the ideal repairer using location based search criteria and view key details of the repairer to allow for smart work allocation</p> <p>Integration with google maps allows the booking agent to visualise the location of the repairer network in relationship to the Asset.</p> <p>Key information including site opening hours, distance to your location, the services the workshop provides and information on any franchises held for those looking to book warranty repairs.</p>			



TECH ASSIST

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
Touch screen interface We've spent a decade optimising the digital capture of service information so it's simple, intuitive and fast. Inspect is optimised for touch screen data entry at source, ensuring better compliance, quality of data and faster processing of documents. By digitising the workflow you can ensure that the quality of your documentation is of the highest standard, is available immediately and your customers will love you.			
Digital workflows Replace all your manual inspection and service forms with simple and intuitive electronic workflows. Inspect enables workers on and off-site to input inspection data directly into a tablet or hand-held computer. This process eliminates paper intensive data collection, reduces input errors and speeds up the information flow.			
Standardise data Workflow instructions by organisational rules criteria. No matter how good your manual processes and quality checks are it's not always possible to standardise outputs. With Inspect you can customise and prescribe the workflow, ensuring a standard way of classifying defects and reporting actions is undertaken by all your engineers. Work instruction guides can be given at the time of data input so engineers know exactly what action is required to be done.			
Built in QA Gone are the days of mucky service sheets with illegible handwriting and missing information. With Inspect you can ensure document accuracy, completeness and legibility with sophisticated business logic checks and procedures to ensure data integrity and completeness.			

CONTACT

r2c Online Limited
2 Vantage Drive
Sheffield
South Yorkshire
S9 1RG, UK

+44 (0)114 399 2430
www.r2conline.com



Vantage Point

Feature List

NOVEMBER 2018



OVERVIEW

Vantage Point is the visual intelligence tool for optimal business efficiency. Use interactive analytics and full top-to-bottom data visibility to take control of your business' next steps. Vantage Point will provide an overview of your current performance data.

Vantage Point also has an Earned Recognition module which can be included as an added extra which provides a measure of a Fleet Operator's compliance and aid in achieving DVSA's Earned Recognition status.

MY VP

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
Key KPI's The r2c Online MyVP view provides an instant view of the 5 most important KPIs for your business' operations at a glance, including MOT Pass Rate, Running Costs, Compliance Currency, Unscheduled Events and Daily Driver Checks.			
Key KPI Analytics The r2c Online MyVP view features the important information that drives the 5 key KPIs which can be viewed with a simple click of the mouse.			

MY FAVOURITES

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
Personalised Favourites r2c Online Vantage Point provides the ability for users to create a dashboard of their favourite Vantage Point charts bringing together information that is important to that user into a one stop location.			

RUNNING COSTS

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
<p>Business Costs</p> <p>With r2c Online Vantage Point you can delve into the world of your business' costs, providing insights such as Spend by Period, Average Job Cost, Average Cost by Manufacturer etc.</p>			
<p>Operational Measures</p> <p>Vantage Point provides users with an insight into operational measures such as Pricing Items by Reason, Parts Volume by Site, Parts Cost by Manufacturer etc.</p>			

COMPLIANCE

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
<p>Compliance Overview</p> <p>The r2c Online Vantage Point compliance overview screen provides the user with important information relating to the compliance of their fleet including MOT Performance, Current VOR status etc.</p>			
<p>MOT Performance</p> <p>With r2c Vantage Point, users can drill down into vital statistics about their business' MOT performance such as Performance Volume, By Depot, By Repair Agent Volume etc..</p>			
<p>Scheduling Analytics</p> <p>r2c Online Vantage Point can provide users with important analytics about their scheduled and unscheduled events for example, Planned vs Unplanned events, Planner Events by Week, Adhoc Events by Manufacturer etc.</p>			
<p>Driver Checks Performance</p> <p>Being compliant is an integral requirement for any fleet operator's business. r2c Vantage Point can help with analysing driver checks, providing essential information such as Checks Completed by Period, Defects raised by Reason, Average driver Check Time etc..</p>			

Features	Workshops	Fleet Operators	Fleet Management
Fleet Configuration Analysis With r2c Online Vantage Point, you can gain an insight into the configuration of your fleet, for example Fleet by Site, Jobs by Fleet Type etc.			
Job Analysis r2c Vantage Point provides key statistics around job volumes by providing important information such as Jobs by Period, Jobs by Fleet Type, jobs by Registration Band etc.			

VOR

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
VOR Performance Understanding your VOR performance is a key aspect of being compliant. r2c Vantage Point provides VOR statistics such as Days Lost to VOR by Period, Average Days Lost to VOR by Period, Total Days Lost to VOR by Reason etc.			

FLEET HEALTH

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
Fleet Quality Analytics Having a healthy fleet allows fleet operators to manage compliance with ease. r2c Vantage Point allows you to find important information about the quality of your fleet data for example, Assets Missing MOT Expiry Date, Assets Missing Service Cycle etc.			

EARNED RECOGNITION

Feature Comparison

Features	Workshops	Fleet Operators	Fleet Management
<p>Earned Recognition Status Overview</p> <p>The Earned Recognition module is an important add-on to those fleet operators who are registered for the DVSA Earned Recognition scheme.</p> <p>With the Earned Recognition module, you can gain an early insight into your fleet's compliance enabling you to rectify any issues that may cause non-compliance.</p> <p>The Earned Recognition Status Overview screen is your 'one stop shop' for everything you need to know about your Earned Recognition status. With vital information such as Next Submission Date, Maintenance KPIs, Earned Recognition Eligible Asset Health Check etc.</p>			
<p>Earned Recognition KPI Drilldowns</p> <p>The Earned Recognition module allows you to drill down into each maintenance KPI giving you the key details you need to monitor for each KPI.</p>			

CONTACT

r2c Online Limited
2 Vantage Drive
Sheffield
South Yorkshire
S9 1RG, UK

+44 (0)114 399 2430
www.r2conline.com

