

# Terms and conditions (Supplier Terms)

Government and Housing: Software as a Service  
(SaaS)

## Structure of these Supplier Terms

These Supplier Terms contain provisions that are specific to the provision of Government & Housing SaaS. At the end of the General Provisions there is an Annex for NEC Local Welfare Provision which sets out additional product/service specific provisions (which also override the General Provisions if there is any conflict). At the end of these Supplier Terms is a Glossary. Any capitalised terms within these Supplier Terms which are not defined in the Glossary shall have the meaning set out elsewhere in this Agreement.

## General Provisions

### Onboarding Services

The Supplier shall deliver the Onboarding Services specified in the Particulars.

Unless expressly stated otherwise in the Particulars, the parties recognise that any Onboarding Services and Professional Service days set out in this Agreement are an estimate based on the parties' current understanding of their requirements and obligations.

Subject to the paragraph below, the Supplier will use reasonable endeavours to accommodate rescheduling of Onboarding Services and Professional Services at the Buyer's request. However, if the Buyer seeks to reschedule or postpone Professional Services or Onboarding Services within: (a) ten to six Working Days of the booked date for delivery, the Supplier shall be entitled to invoice the Buyer for 50% of the relevant charges; or (b) five Working Days or less of the booked date for delivery, the Supplier shall be entitled to invoice the Buyer for 100% of the relevant Charges. All days paid for must be utilised within 12 months of the date of the Buyer's Purchase Order.

If the Buyer seeks to postpone Onboarding Services or Professional Service days at any time where the Supplier has booked a flight or incurred other reasonable expenses which are non-refundable, the Buyer will still be liable to pay the cost of such flight or other expenses.

Unless expressly stated otherwise in the Particulars, all SaaS shall be tested in accordance with the Supplier's standard test policies. Any additional testing activities that the Buyer requires the Supplier to carry out must be agreed in writing between the parties and may be chargeable. The Buyer shall be deemed to accept the SaaS, and such acceptance shall be irrevocable, if the SaaS is used by the Buyer in a live environment and/or for any live operations.

### Access to and use of the SaaS

Subject to the Buyer complying with the restrictions set out in these Supplier Terms and the other terms and conditions in this Agreement, the Supplier shall grant to the Buyer a non-exclusive, non-transferable right to permit the Authorised Users to use the SaaS and the Documentation during the SaaS Term solely for the Buyer's internal business purposes. The Supplier shall grant the Buyer's Administrator access to the SaaS in the technologically appropriate manner either by provision of a licence key, by granting access to a downloadable app, or by means of issuing a user name and password for the SaaS portal which can be accessed through such URL as may be notified by the Supplier from time to time ("**SaaS Portal**").

The Buyer's Administrator shall then be permitted to access the SaaS through the SaaS Portal and it shall be the Buyer's Administrator's responsibility to configure the set-up of

the SaaS, within the parameters set out within the Documentation, to reflect the Buyer's own policies and practices on application assessment and decision making.

The Buyer's Administrator, in accordance with the Documentation, shall be permitted to set up further users authorised to access the SaaS on behalf of the Buyer up to the numerical limit specified in the Particulars (if applicable). It is the Buyer's Administrator's responsibility to set the controls on and levels of access for each further user authorised. For the avoidance of doubt, the Buyer's Administrator and the further users set up by the Buyer's Administrator under this paragraph shall be the "Authorised Users" for the purposes of this Agreement.

- If there is an End User named in the Particulars, the Supplier grants the Buyer the right to access and use the SaaS for the benefit of such End User.

In relation to the Authorised Users, the Buyer undertakes that:

- Each Authorised User shall keep a secure password for his/her use of the SaaS and Documentation, that such password shall be kept confidential and shall be changed no less frequently than every 90 days;
- It shall maintain a written, up to date list of the current Authorised Users and provide such list to the Supplier within five Working Days of the Supplier's written request at any time or times;
- It shall permit the Supplier to audit the SaaS. Such audit may be conducted no more than once per quarter, at the Supplier's expense, and this right shall be exercised with reasonable prior notice, in such a manner as not to substantially interfere with the Buyer's normal conduct of business. If any of the audits referred to in this paragraph reveal that any unauthorised access has occurred, then without prejudice to the Supplier's other rights, the Buyer shall promptly disable such accounts.

In relation to the Buyer's Administrator, the Buyer undertakes that:

- The Buyer's Administrator will review and act upon any update information or reasonable instructions of the Supplier, including disseminating such applicable update information and instructions to other Authorised Users; and
- The Buyer's Administrator shall monitor the Authorised Users and ensure that they act in accordance with the terms of this Agreement.

The Buyer and its Authorised Users shall not access, store, distribute or transmit any Viruses, or any material during the course of its use of the SaaS that:

- Is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;
- Facilitates illegal activity;
- Depicts sexually explicit images;
- Promotes unlawful violence;
- Is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or
- Is otherwise illegal or causes damage or injury to any person or property;
- And the Supplier reserves the right, without liability or prejudice to its other rights to the Buyer, to disable the Buyer's access to any material that breaches the provisions of this paragraph.

The Buyer and its Authorised Users shall not:

- Attempt to reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the SaaS, except:
  - ➔ As may be allowed by any applicable law which is incapable of exclusion by agreement between the parties; and
  - ➔ To the extent expressly permitted under this Agreement;
- Attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the SaaS and/or Documentation (as applicable) in any form or media or by any means; or
- Access all or any part of the Services and Documentation in order to build a product or service which competes with the SaaS and/or the Documentation; or
- Use the SaaS and/or Documentation to provide services to third parties (the Buyer's citizens shall not be deemed to be third parties for the purposes of this paragraph); or
- License, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the SaaS and/or Documentation available to any third party except the Authorised Users, or
- Attempt to obtain, or assist third parties in obtaining, access to the SaaS and/or Documentation, other than as provided under this paragraph.

The Buyer shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the SaaS and/or the Documentation and, in the event of any such unauthorised access or use, promptly notify the Supplier.

The Buyer shall access the SaaS by network communications as agreed between the parties.

The Supplier will use reasonable commercial endeavours to accommodate the introduction of legislative changes. The Supplier expressly reserves the right to charge for the provision of any such legislative updates where: (a) the development of the update is in the reasonable opinion of the Supplier technically complex; and (b) the costs of developing the update are in the reasonable opinion of the Supplier sufficient to warrant a charge for the provision of the update to the Supplier's buyers at large.

## Security, Disaster Recovery and Back-up Policy

The Buyer shall own all right, title and interest in and to all of the Buyer Data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of the Buyer Data.

The Supplier confirms that:

- The SaaS is provided via a private community cloud for the sole use by or on behalf of the public sector;
- The SaaS platform is designed and implemented in accordance with the 27001 baseline control set and the 14 Cloud Security Principles from the National Cyber Security Centre (NCSC) guidance. The environment from which the SaaS shall be delivered conforms to the relevant sections of the Government Security Policy Framework and Personnel Security Controls and to all relevant Communications Electronics Security Group Memoranda, Manuals and Standards;
- It shall comply with the Supplier's Privacy and Security Policy relating to the privacy and security of the Buyer Data;

- Its information security management system is certified to ISO 27001 and ISO 27002;
- Its quality management system is certified to ISO 9001:2015 (TickIT);
- Its service management system operates in accordance with ISO 20000-1:2018; and
- The information assurance process as detailed within the paragraphs above will be periodically revised and updated to ensure alignment with good industry practice.

The Buyer recognises that the SaaS is a hosted, multi-tenanted solution. The Buyer Data will be segregated from the data of other Supplier buyers using the SaaS and there will be no data sharing facility unless expressly authorised by the Buyer.

The Supplier confirms that it uses more than one data centre with separate infrastructure and resilience for provision of the SaaS to ensure relocation of the SaaS provision in the event of non-availability of one data centre.

The Supplier confirms that its disaster recovery and business continuity policies, processes and procedures are based on standard BS25999 and ISO 22301:2019.

The Back-Up Policy is as follows:

- The Supplier takes multiple back-ups within the system as part of the SaaS, in particular, back-ups are taken daily from the live system utilising an automated process scheduled to run overnight, taking into account any batch routines and system availability requirements;
- Back-ups are stored at a different location to the live service;
- In the event of any loss or damage to Buyer Data, the Buyer's sole and exclusive remedy shall be for the Supplier to use reasonable commercial endeavours to restore the lost or damaged Buyer Data from the latest back-up of such Buyer Data maintained by the Supplier; and
- The Supplier shall not be responsible for any loss, destruction, alteration or disclosure of Buyer Data caused by any third party (except those third parties sub-contracted by the Supplier to perform services related to Buyer Data maintenance and back-up).

## Buyer Obligations

Except where the Supplier has specifically agreed to provide such services the Buyer will:

- Be responsible for the operation and use of the SaaS and any associated documentation and the results obtained from these; and
- Supply the Supplier with any information and assistance reasonably necessary for the Supplier to perform its obligations under this Agreement.

The Buyer shall in good faith:

- Provide the Supplier with (i) all necessary co-operation in relation to this Agreement; and (ii) all necessary access to such information as may be required by the Supplier in order to provide the SaaS, including but not limited to Buyer Data;
- Comply with all applicable laws and regulations with respect to its activities under this Agreement;
- Carry out all other Buyer responsibilities set out in this Agreement in a timely and efficient manner. In the event of any delays in the Buyer's provision of such

assistance as agreed by the parties, the Supplier may adjust any agreed timetable or delivery schedule as reasonably necessary and reserves the right to charge the Buyer for any costs incurred by the Supplier as a consequence of such delay;

- Ensure that (where applicable) the Authorised Users use the SaaS and the Documentation in accordance with the terms and conditions of this Agreement and shall be responsible for any Authorised User's breach of this Agreement;
- Obtain and shall maintain all necessary licences, consents, and permissions necessary for the Supplier, its contractors and agents to perform their obligations under this Agreement, including without limitation the SaaS;
- Ensure that its network and systems comply with the relevant specifications provided by the Supplier from time to time; and
- Be solely responsible for procuring and maintaining its network connections and telecommunications links from its systems to the Supplier's data centres, and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the Buyer's network connections or telecommunications links or caused by the internet.

## SaaS Availability and Support

The Supplier shall use commercially reasonable endeavours to make the SaaS available 08:00 to 20:00 on Working Days, except for:

- Planned maintenance carried out during the maintenance window of (i) 18:00 to 08:00 on a Working Day; and (ii) at any time on a non-Working Day, for which the Supplier shall give the Buyer at least 24 hours' notice in advance; and
- Unscheduled emergency maintenance carried out, where possible unless there is an identified and demonstrable immediate risk to the SaaS infrastructure, during the maintenance window of (i) 18:00 to 08:00 on a Working Day; and (ii) at any time on a non-Working Day, for which the Supplier shall use reasonable endeavours to give the Buyer at least six hours' notice in advance.

The SaaS supports mainstream browsers for example IE (Edge), Chrome, Firefox and Safari unless otherwise stated in the release documentation.

During the SaaS Term the Supplier shall, as part of the SaaS and at no additional cost to the Buyer, provide the Buyer with the Supplier's standard Buyer support services through its service desk ("Service Desk").

The Service Desk can be contacted by the Buyer's Authorised Users via the Supplier's customer portal which can be accessed through the URL [www.customersupport.necsws.com](http://www.customersupport.necsws.com) ("Customer Portal"), 24 hours a day, seven days a week.

When logging a request for support ("Support Request"), the Authorised User must provide the following information to the Service Desk (whether through the Customer Portal or over the telephone):

- Authorised User Name;
- Authorised User Location;
- Authorised User's contact details – telephone and email;
- Details of the nature of the fault or description of the issue; and



- Details of who is being affected, i.e. single user, a group of users or the whole organisation, and the impact that the fault or issue is having including any urgency surrounding the support call.

Upon receiving a Support Request but in any event within four hours during Working Hours, the Service Desk will prioritise the call as set out below:

Prioritisation of Incidents	
Priority	Description
1	<ul style="list-style-type: none"> <li>• Service non-functional with high impact on Authorised User operations.</li> <li>• Complete loss of a critical business function at a critical time in the business cycle.</li> <li>• Security breach.</li> </ul>
2	<ul style="list-style-type: none"> <li>• Partial loss of a business function at a critical time in the business cycle with medium impact on Authorised User operations.</li> <li>• Complete loss of a business function at a non-critical time.</li> <li>• Performance degradation affecting 25% or more of Authorised Users.</li> </ul>
3	<ul style="list-style-type: none"> <li>• Minor problems with very low impact on Authorised User operations where processing can continue.</li> <li>• Performance degradation affecting less than 25% of Authorised Users.</li> </ul>
4	<ul style="list-style-type: none"> <li>• Service Requests.</li> </ul>

The Supplier will commence working towards a resolution of the Incident once accepted and shall use reasonable endeavours to resolve Incidents in accordance with the following Response and Resolution Table:

Response and Resolution Table		
Priority	Target time to Respond	Target time to Resolution
1	15 Working Minutes	4 Working Hours
2	30 Working Minutes	8 Working Hours
3	60 Working Minutes	36 Working Hours
4	1 Working Day	As agreed

**"Target time to Respond"** in the Response and Resolution Table above shall mean the target time taken for acknowledgement of receipt of the Incident either by phone or electronically via email, provision of an Incident reference number and allocation of a priority in accordance with the Incident Priority Table.

Unresolved Incidents will be escalated by the Buyer with the Supplier personnel in the following order:

- Supplier CSM (if applicable); then
- Supplier Client Services Director; then
- Supplier Operations Director.

Where, in the reasonable opinion of the Supplier, the Resolution of an Incident is not possible due to the ability to Resolve such Incident being outside the Supplier's control, the Supplier shall formally notify the Buyer accordingly and the parties shall agree appropriate remedial action, such agreement not to be unreasonably withheld, and in these instances no Hosting Service Credits shall apply.

Where multiple Incidents are related to the same occurrence of an issue within the same 24 hour period they will be linked to the original Incident and shall only count as one Incident for the purposes of service measurement.

Subject to the paragraph immediately below, the Service Desk will contact the Authorised User detailed in the Support Request during Working Hours and conduct an initial analysis in order to try and resolve operational issues and minor technical issues directly with the Authorised User within the call. Where it is not possible to resolve the Support Request within the call, the Authorised User will be notified and the Support Request will be escalated to the relevant technical team.

The Supplier shall have no obligation to:

- Correct any error reported by the Buyer if such reported error is not reproducible by the Supplier in the SaaS;
- Correct any Priority 4 reported errors and reserves the right to abandon attempts to provide a fix where the costs are likely to be excessive or the commercial benefits to the Supplier's customers at large are likely to be negligible; or
- Correct any error if such error arises from misuse or abuse of the SaaS.

## Termination and Consequences of Termination

In the event the Supplier elects to withdraw a particular type of SaaS, it may do so without liability provided it has given the Buyer not less than six months' prior written notice. The Supplier shall, following the expiry of the SaaS Term, disable the Buyer's access to the SaaS.

## Miscellaneous

- If this Agreement contains the Buyer's service description, requirements or specification ("**Specification**") and if any provision of that Specification conflicts with these Supplier Terms, then regardless of any other provision in this Agreement, these Supplier Terms will take precedence.
- Regardless of any other provision in this Agreement, except to the extent not permitted by law:
  1. the Buyer assumes sole responsibility for results obtained from its use of the Supplier's deliverables and for any conclusions drawn from such use; and
  2. the Supplier shall have no liability for any damage caused by errors or omissions in any information, data, instructions or scripts provided to the Supplier by the Buyer in connection with this Agreement, or any actions taken by the Supplier at the Buyer's direction.
- Except where the Supplier has specifically agreed to provide such services, the Buyer will promptly:



1. supply the Supplier with any information and assistance reasonably necessary for the Supplier to perform its obligations under this Agreement; and
  2. provide the Supplier's personnel with full free and safe access to its site when required, to enable the Supplier to perform its obligations under this Agreement.
- The Buyer warrants, represents and undertakes to the Supplier that there will be no relevant transfer for the purposes of the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ("**TUPE**") of employees from the Buyer (or any supplier, contractor or other service provider to the Buyer) to the Supplier. Regardless of any other provision of this Agreement, the Buyer agrees to indemnify the Supplier against all costs, claims, liabilities and expenses (including reasonable legal expenses) incurred by the Supplier in connection with or as a result of:
    1. a claim by any person who transfers or alleges that they have transferred to the Supplier as a result of entering into this Agreement; and/or
    2. any failure by the Buyer to comply with its obligations under regulations 13 and 14 of TUPE, or any award of compensation under regulation 15 of TUPE.

## Annex: Local Welfare Provision (“**LWP**”) and LWP Reporting

Where LWP SaaS is to be provided the provisions set out in this Annex shall apply. If there is any conflict between the provisions set out in this Annex, and any other provisions set out in these Supplier Terms, this Annex shall apply:

### Onboarding Services

The Supplier shall provide remote services to the Buyer to demonstrate the configurability and day to day use of LWP.

### Data Storage Space

The Supplier confirms that LWP does not place any limit on the amount of data storage space available to the Buyer as part of the Charges.

### Termination and Consequences of Termination

The Supplier confirms that not less than 10 Working Days after the expiry or earlier termination of this Agreement (or such other date as may be agreed between the parties where data extraction services have been agreed in accordance with these Supplier Terms) the Supplier shall delete and remove from the live LWP system and infrastructure the Buyer Data. For the avoidance of doubt, the Supplier shall be permitted to retain a copy of the Buyer Data for a period of up to 12 months for the purposes of audit.

### Off-Boarding and Data Extraction

If the Buyer would like to extract any or all of their Buyer Data in a different manner outside of the standard reporting suite available within LWP upon the expiry or earlier termination of this Agreement, then the Buyer must give the Supplier a minimum of two months written notice prior to the date of the expiry or earlier termination, whereupon the Buyer and the Supplier shall agree the scope of the Buyer Data to be extracted together with the format of the extracted Buyer Data and associated costs.

Following any extraction of Buyer Data as agreed between the parties in accordance with these Supplier Terms, as stated above, all Buyer Data will be deleted.

### Miscellaneous

The Buyer shall access LWP by means of a Government Secure Network connection only and it shall be the Buyer’s responsibility to obtain and maintain its own Government Secure Network connection.

# Glossary

In addition to the terms defined elsewhere in these Supplier Terms (or other parts of the Agreement), the following terms shall have the following meaning:

"Agreement"	means the Call-Off Agreement.
"Authorised Users"	means those employees, agents and independent contractors of the Buyer who are authorised by the Buyer to use the SaaS and the Documentation, as further described in these Supplier Terms.
"Back-Up Policy"	means the specific arrangements for the back-up of Buyer Data as set out in these Supplier Terms, as may be amended from time to time by the Supplier in its sole discretion upon reasonable prior written notice.
"Buyer's Administrator"	means the person duly appointed by the Buyer to act as its administrator and the Supplier's lead contact for the purposes of the SaaS, as notified by the Buyer to the Supplier.
"Buyer Data"	means the data inputted by the Buyer, or Authorised Users for the purpose of using the SaaS or facilitating the Buyer's use of the SaaS.
"End User"	means the entity identified as such in the Particulars.
"Particulars"	means the Order Form.
"Privacy and Security Policy"	means the Supplier's policy relating to the privacy and security of the Buyer Data, as may be amended from time to time by the Supplier in its sole discretion, which is available on request.
"SaaS"	means the Software as a Service to be delivered as set out in the Particulars.
"SaaS Portal"	has the meaning set out in these Supplier Terms.
"Virus"	means any thing or device (including any software, code, file or program) which may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any program or data, including the reliability of any program or data (whether by re-arranging, altering or erasing the program or data in whole or part or otherwise); or adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices.

"Working Day"	means any day which is not a Saturday, Sunday or bank or public holiday in the UK. All references to hours within a Working Day are to UK hours.
"Working Hours"	means 09:00 to 17:30 UK time, each Working Day.
"Working Minutes"	means minutes within a Working Hour.



About NEC Software Solutions

Our customers change lives, so we create software and services that get them better outcomes. By innovating when it matters most, we help to keep people safer, healthier and better connected worldwide.

NECSWS.com

**NEC**

1st Floor, Bizspace, iMex Centre,  
575-599 Maxted Rd,  
Hemel Hempstead HP2 7DX  
+44 (0)1442 768445