

# Terms and conditions (Supplier Terms)

Safety: Software as a Service (SaaS)

## Structure of these Supplier Terms

These Supplier Terms contain provisions that are specific to the provision of SaaS. At the end of these Supplier Terms there are also a number of product-specific Annexes, which set out additional product/service specific provisions (which also override the General Provisions if there is any conflict). Only the Annexes which relate to the SaaS purchased by the Buyer (as set out in the Particulars) shall apply. There are Annexes for:

- NEC Interventions Manager
- NEC Media Manager
- NEC Pathways Youth Offending CMS and NEC Pathways CMS
- Stream
- NEC Connect SaaS
- NEC Virtual Interviewer
- NEC Hearings Manager

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

### Introduction

“**SaaS**” means software as a service. Each buyer which subscribes for the Supplier’s SaaS is given a right of access to the Supplier’s applicable proprietary application software (“**Software**”), via the internet or a private network, for the duration of the SaaS Term. Buyers are not granted a licence to the Software. The Software is hosted either in the Supplier’s private cloud or a third party’s public cloud. The Supplier’s SaaS solutions:

- Always run on the latest version of the Software;
- Unless otherwise stated in the product-specific Annex, are multi-tenanted which means many buyers using the same executables and database;
- Run on a single version of the Software which used by all SaaS buyers; and
- Comprise the right to use the Software and the Documentation and the right to access Software support services, as described below. The Buyer does not have to host the Software or install it on its own premises/hardware.

Where the Software is not delivered as SaaS but is delivered via a private cloud (an on-premise, or separately procured, private cloud), alternative provisions set out in the Supplier Terms for (i) Licence Terms and (ii) Safety Support and Maintenance shall apply.

## Onboarding Services for SaaS

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 Business 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 Business 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 stipulated 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.

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; and
- 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 paragraph above shall not apply to the extent only that the SaaS is specifically designed for such purposes and is being used lawfully including for the prevention and/or detection of criminal activity.

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 substantive legislative changes. The Supplier expressly reserves the right to charge for the provision of any such substantive 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.

Unless otherwise expressly stated in an Annex in relation to a particular SaaS product, the Supplier confirms that:

- The SaaS platform is designed and implemented in accordance with the 27001 baseline control set, the 14 Cloud Security Principles and 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 9001:2008 (TickIT);
- Its service management system operates in accordance with the ITIL framework;
- It conducts annual IT health checks including penetration testing with an independent CHECK consultant. Reports from such IT health checks will be shared with the Buyer; 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 unless stated otherwise in the product-specific Annex. The Buyer Data will be segregated from the data of other buyers using the SaaS and there will be no data sharing facility.

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 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;
- Supply the Supplier with any information and assistance reasonably necessary for the Supplier to perform its obligations under this Agreement; and
- Provide the Supplier's personnel with full free and safe access to its site where required, to enable 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 and security access information;
- 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
- Unless expressly stated otherwise in the Particulars, be solely responsible for procuring and maintaining its network connections and telecommunications links from its systems to the Supplier's public or private cloud (as applicable), 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 Support Services

The Buyer's Support Team shall provide the following services:

- Infrastructure support up to the Supplier SaaS boundary
- Receive Calls from Authorised Users
- Apply the Buyer's service management processes
- Request Fulfilment (i.e. respond to Service Requests) comprising:
  - System administration
  - Application configuration including CV lists, creation of users
  - Deal with "how do I?" enquiries
  - Configure additional users
- Incident Management comprising:
  - Address data quality issues
  - Observe and accurately record symptoms of an Incident including any testing and subsequent results
  - Triage Incidents to establish that the Supplier SaaS is the likely cause of an Incident
  - Carry out work on-site to assist the Supplier Support Team in further diagnostics
  - Simple investigation and Resolution using diagnostic tools / log files
  - Facilitate Resolution by switching to a standby system (if applicable) or from backups or implement a temporary work-around and continue work to apply a permanent Resolution
  - Notify the Supplier of any Incident which has been resolved and the steps taken to resolve
- Knowledge Management comprising:
  - Application of available knowledge
  - Generation and maintenance of knowledge articles

Should the Buyer's Support Team be unable to resolve an Incident or fulfil a Service Request, a Call shall be logged with the Supplier. During the SaaS Term the Supplier

shall, as part of the SaaS and at no additional cost to the Buyer, provide the Buyer's Support Team access to the Service Desk which operates 24x7x365 for recording details of Calls. The Buyer's Support Team can use the following methods to contact the Service Desk:

- Telephone (Priority Levels P1, P2, P3, P4 and Service Request);
- Supplier's Customer Portal (Priority Level P3, P4 and Service Request); and
- Email (Priority Level P3, P4 and Service Request).

When contacting the Service Desk to report a Call, the Buyer's Support Team shall provide the following information:

- Caller name (and further contact details if required);
- Name and contact details of the Authorised User experiencing the issue (if applicable);
- Priority;
- A description of the issue including the steps to replicate; and
- A description of the urgency and impact of the issue.

Once these details have been entered into the Supplier's IT service management tool, the Supplier will provide the Buyer's Support Team with a Call reference number, which shall be quoted by the Buyer's Support Team in all further communication with the Supplier in connection with the Call.

Once Calls have been logged, they are passed to a software support team for Resolution (the "**Supplier Support Team**") during Normal Support Hours.

At any stage during the lifecycle of a Call the Buyer's Support Team can enquire on progress status by contacting the Service Desk and quoting the relevant Call reference number.

The Supplier Support Team shall provide:

- Remote support services as detailed in these Supplier Terms;
- New Releases, which may be subject to additional charges;
- Software Patches to resolve incidents/problems; and
- Service Packs as they are made generally available which may be subject to an additional charge if they include new functionality.

The provision of the Support Services is subject to the Buyer providing such information as is reasonably necessary to enable the Supplier to diagnose any Incidents or Problem in the Supplier SaaS.

## Service Levels

Calls logged with the Service Desk will be allocated to the Supplier Support Team for Resolution during Normal Support Hours. The Particulars shall specify whether 24x7 support for P1 and P2 Incidents shall apply

Incidents and Service Requests are processed on a Priority Level basis. The Supplier will verify the Priority Level assigned by the Buyer's Support Team on the Call, by reference to the applicable Annex, and the parties will agree a revised Priority Level if appropriate. The final decision on the Priority Level will remain with the Supplier.

In order to perform Incident investigation and Service Request fulfilment, the Supplier may require access to the Authorised User experiencing the issue. The Buyer shall promptly provide such access as and when reasonably requested.

As Calls are progressed, the Supplier will record details of all its contact with the Buyer's Support Team and/or Authorised User.

Once a Call has been resolved, the Supplier Support Team or Service Desk will contact the Buyer's Support Team and the Call will only be closed if both parties are in agreement. Closed Calls cannot be reopened except with the consent of both parties. Should the Supplier not receive confirmation of closure after seven calendar days of requesting the same from the Buyer's Support Team, then the Supplier will automatically close the Incident.

When a Problem is identified which requires a change to the SaaS solution, a Problem will be recorded and a reference number supplied to the Buyer's Support Team; this needs to be quoted in all correspondence with the Supplier relating to that Problem. The corresponding Incident is then closed if a workaround is provided.

Measurement of the Response time begins at the earliest point in time during Normal Support Hours at which the Call is reported to the Service Desk, and will continue during Normal Support Hours. If a Call is reported outside of Normal Support Hours, the Response time will start to be measured at the beginning of the next Normal Support Hours period. Measurement of the Response time ends when the Supplier has contacted or attempted to contact, via any means, the Buyer's Support Team to acknowledge receipt of or further discuss a reported Call.

Measurement of the Resolution time begins at the earliest point in time during Normal Support Hours at which the Call is reported to the Service Desk, and will continue during Normal Support Hours. If a Call is reported outside of Normal Support Hours, the Resolution time will start to be measured at the beginning of the next Normal Support Hours period. Measurement of the Resolution time ends when the Incident has been resolved and the workaround or permanent fix provided to the Buyer, or the Service Request has been fulfilled (as applicable).

The Supplier SLA clock is paused in certain circumstances including:

- While the Call is outside the scope or control of the Supplier; and
- Outside Normal Support Hours; and
- While the Supplier is awaiting information from the Buyer's Support Team or Authorised User.

In addition, should Supplier personnel be required to attend site, this will be charged for on a time and materials basis in accordance with the rate card set out in the contract (or if none included in accordance with the Supplier's prevailing rates) plus expenses.

The Supplier will not be liable for any service failure:

- For which the Supplier is not responsible; or
- Which relates to an Additional Service; or
- Which arises as a result of Incidents arising due to factors beyond the Supplier's reasonable control.

The Supplier shall use commercially reasonable endeavours to make the SaaS available to be accessed and used by the Buyer 99.9% of the time, measured during Normal Support Hours, excluding the following periods:

- Planned maintenance (which shall be carried out at such times as are notified to the Buyer, by giving a reasonable period of advance notice); and
- Unscheduled emergency maintenance carried out where there is an identified and demonstrable immediate risk to the SaaS solution.

Service credits shall not apply in the event of breach of the Service Levels.

Service reporting is not provided as part of SaaS.

## Additional Services

Additional Services shall be provided at the Supplier's sole discretion and may be subject to additional charges accruing on a time and materials basis based on the Supplier's then prevailing day rates, unless otherwise agreed. Such Additional Services include:

- The provision of health checks either monthly, quarterly or annually;
- The provision of service reporting
- Engagement with respect to a business continuity or disaster recovery testing;
- Attendance on Buyer's site to investigate and resolve an incident or problem;
- Investigation and Resolution of an Incident reported by the Buyer if such reported Incident is not reproducible by the Supplier in the SaaS; and
- Investigate and resolve any Priority 4 Incidents or Problems where costs are likely to be excessive or the commercial benefits to the Supplier's customers at large are likely to be negligible.

The Support Services shall not include the diagnosis or rectification of any Incident which is not attributable to a Problem in the SaaS or which results from any of the following, the diagnosis or rectification of which shall all be considered Additional Services:

- Improper use, operation or neglect of either the SaaS or the equipment and environment on which the Supplier Software is licensed for use; or
- Modification of the SaaS or its merger (in whole or in part) with any other software, without the Supplier's prior written consent; or
- Use of the SaaS on equipment other than the equipment supplied by the Supplier for use with the SaaS or on equipment which does not meet the minimum specification for hardware, operating system and/or Third Party Software published by the Supplier in accordance with the SaaS release information document; or
- Failure by the Buyer to implement recommendations in respect of or solutions to Incidents or Problems previously advised by the Supplier; or
- Any repair, adjustment, alteration or modification of the SaaS by any person other than the Supplier without the Supplier's prior written consent; or
- Use of the SaaS for a technical purpose for which it was not designed; or
- A consequence of infrastructure components or network factors which the Supplier is not responsible for supporting; or
- A failure caused by any other factors outside the reasonable control of the Supplier; or

- Any situation where a reasonably skilled and competent Authorised User would consider assistance from the Supplier to be unnecessary; or
- A consequence of any programming error, virus or disabling code set out in the Third Party Software; or
- Use of SaaS on anything other than Edge or Chrome browsers, unless otherwise stated in the release documentation.

## Variations

If a third party supplier to the Supplier increases the fees charged, the Supplier reserves the right at any time to pass these increases onto the Buyer.

The Supplier may, upon six months' prior written notice to the Buyer, modify the SaaS or any part thereof provided that there is no material degradation of the service.

## 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:
  - 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
  - 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:
  - Supply the Supplier with any information and assistance reasonably necessary for the Supplier to perform its obligations under this Agreement; and
  - 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:

- 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
- 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: NEC Interventions Manager

Where NEC Interventions Manager 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 the General Provisions above, this Annex shall apply.

### Use of a third party's public cloud

The Buyer consents to the use of AWS as a sub-processor of personal data for the purpose of providing AWS cloud services, and acknowledges and agrees to the provision of those services on AWS' standard terms.

### Service Levels

All target times specified in the table below are measured within the Normal Support Hours.

Service Levels for NEC Interventions Manager			
Call Priority Level	Definition	Target Response Time	Target Resolution Time
P1	Critical. Comprising: The system is unavailable to all Authorised Users. Performance degraded to such an extent that NEC Interventions Manager is unable to be used by all users.	30 minutes	4 hours
P2	High. Comprising: Loss of a major area of functionality impacting all Authorised Users. Performance of a major area of functionality is degraded such that the business process cannot be delivered, and is affecting all Authorised Users.	2 hours	1 day
P3	Medium. Comprising: An important business function of the system is affecting a group of Authorised Users.  Loss of an area of functionality impacting a group of Authorised Users. Performance of an area of functionality is degraded for a group of Authorised Users such that they are unable to deliver the business process.	4 hours	3 days
P4	Low. Comprising: Issue affecting a single Authorised User	24 hours	5 days
Service Request	For example: requests for information, advice and/or guidance.	None	None

## Annex: NEC Media Manager

Where NEC Media Manager 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 the General Provisions above, this Annex shall apply.

### Use of a third party's public cloud

The Buyer consents to the use of AWS as a sub-processor of personal data for the purpose of providing AWS cloud services, and acknowledges and agrees to the provision of those services on AWS' standard terms.

### Service Levels

All target times specified in the table below are measured within the Normal Support Hours.

Service Levels for NEC Media Manager			
Call Priority Level	Definition	Target Response Time	Target Resolution Time
P1	Critical. Comprising: The system is unavailable to all Authorised Users. Performance degraded to such an extent that the NEC Media Manager is unable to be used by all users.	30 minutes	4 hours
P2	High. Comprising: Loss of a major area of functionality impacting all Authorised Users. Performance of a major area of functionality is degraded such that the business process cannot be delivered, and is affecting all Authorised Users.	2 hours	1 day
P3	Medium. Comprising: An important business function of the system is affecting a group of Authorised Users. Loss of an area of functionality impacting a group of Authorised Users. Performance of an area of functionality is degraded for a group of Authorised Users such that they are unable to deliver the business process.	4 hours	3 days
P4	Low. Comprising: Issue affecting a single Authorised User	24 hours	5 days
Service Request	For example: requests for information, advice and/or guidance.	None	None

## Annex: NEC Pathways Youth Offending CMS and NEC Pathways CMS (together, "Pathways SaaS")

Where Pathways 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 the General Provisions above, this Annex shall apply.

### Use of a third party's public cloud

The Buyer consents to the use of AWS as a sub-processor of personal data for the purpose of providing AWS cloud services, and acknowledges and agrees to the provision of those services on AWS' standard terms.

### Service Levels

All target times specified in the table below are measured within the Normal Support Hours.

Service Levels for Pathways SaaS			
Call Priority Level	Definition	Target Response Time	Target Resolution Time
P1	Critical. Comprising: The system is unavailable to all Authorised Users. Performance degraded to such an extent that the Pathways SaaS is unable to be used by all users.	30 minutes	4 hours
P2	High. Comprising: Loss of a major area of functionality impacting all Authorised Users. Performance of a major area of functionality is degraded such that the business process cannot be delivered, and is affecting all Authorised Users.	2 hours	1 day
P3	Medium. Comprising: An important business function of the system is affecting a group of Authorised Users. Loss of an area of functionality impacting a group of Authorised Users. Performance of an area of functionality is degraded for a group of Authorised Users such that they are unable to deliver the business process.	4 hours	3 days
P4	Low. Comprising: Issue affecting a single Authorised User	24 hours	5 days

Service Request	For example: requests for information, advice and/or guidance.	None	None
-----------------	--	------	------

## Annex: Stream

Where Stream 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 the General Provisions above, this Annex shall apply.

### Use of a third party's public cloud

The Buyer consents to the use of Microsoft Azure as a sub-processor of personal data for the purpose of providing Microsoft Azure cloud services, and acknowledges and agrees to the provision of those services on Microsoft Azure's standard terms.

### Service Levels

All target times specified in the table below are measured within the Normal Support Hours.

Service Levels for Stream			
Call Priority Level	Definition	Target Response Time	Target Resolution Time
P1	Critical. Comprising: The system is unavailable to all Authorised Users. Performance degraded to such an extent that the Stream is unable to be used by all users.	15 minutes	5 hours
P2	High. Comprising: Loss of a major area of functionality impacting all Authorised Users. Performance of a major area of functionality is degraded such that the business process cannot be delivered, and is affecting all Authorised Users.	15 minutes	1 day
P3	Medium. Comprising: An important business function of the system is affecting a group of Authorised Users. Loss of an area of functionality impacting a group of Authorised Users. Performance of an area of functionality is degraded for a group of Authorised Users such that	2 hours	2 days

<b>Service Levels for Stream</b>			
<b>Call Priority Level</b>	<b>Definition</b>	<b>Target Response Time</b>	<b>Target Resolution Time</b>
	they are unable to deliver the business process.		
P4	Low. Comprising: Issue affecting a single Authorised User	2 hours	5 days
Service Request	For example: requests for information, advice and/or guidance.	None	None

## Annex: NEC Connect SaaS

Where NEC Connect 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 the General Provisions above, this Annex shall apply.

### Use of a third party's public cloud

Where stated in the Order Form, the Buyer consents to the use of a third party as a sub-processor of personal data for the purpose of providing cloud services, and acknowledges and agrees to the provision of those services on such third party's standard terms.

### Service Levels

All target times specified in the table below are measured within the Normal Support Hours.

Service Levels for NEC Connect SaaS			
Call Priority Level	Definition	Target Response Time	Target Resolution Time
1	<p>Business Critical. Comprising:</p> <p>Total loss of the NEC Connect SaaS impacting all Authorised Users. Performance degraded to such an extent that the entire NEC Connect SaaS is unable to be used by all Authorised Users.</p> <p>For example: complete live system failure, all Authorised Users unable to access system.</p>	15 Minutes	4 Hours
2	<p>High. Comprising:</p> <p>Loss of a major area of functionality impacting all Authorised Users. Performance of a major area of functionality is degraded such that the business process cannot be delivered, and is affecting all Authorised Users.</p> <p>For example: All Authorised Users are unable to use Case or Custody or Intelligence modules.</p>	30 Minutes	12 Hours
3	<p>Medium. Comprising:</p> <p>Loss of an area of functionality impacting a group of Authorised Users. Performance of an area of functionality is degraded for a group of Authorised Users such that they are unable to deliver the business process.</p> <p>For example: Some Authorised Users are unable to use Case or Custody or Intelligence modules.</p>	4 Hours	24 Hours
4	Low.	4 Hours	48 Hours

	<p>Authorised Users are able to use the NEC Connect SaaS to fulfil the core business process. It could be cosmetic in nature or an activity that is not routinely used such as account management.</p> <p>For example: unavailability of System Administration functions. A single user is experiencing an issue.</p>		
Service Request	<p>Pre-approved low risk change, the nature of which has been agreed by the parties prior to go-live or via the change process.</p> <p>For example: advice and guidance.</p>	None	None

## Annex: NEC Virtual Interviewer

Where NEC Virtual Interviewer 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 the General Provisions above, this Annex shall apply.

### Use of a third party's public cloud

The Buyer consents to the use of AWS as a sub-processor of personal data for the purpose of providing AWS cloud services, and acknowledges and agrees to the provision of those services on AWS' standard terms.

### Service Levels

All target times specified in the table below are measured within the Normal Support Hours.

Service Levels for NEC Virtual Interviewer			
Call Priority Level	Definition	Target Response Time	Target Resolution Time
P1	Critical. Comprising: The system is unavailable to all Authorised Users. Performance degraded to such an extent that NEC Virtual Interviewer is unable to be used by all users.	30 minutes	4 hours
P2	High. Comprising: Loss of a major area of functionality impacting all Authorised Users. Performance of a major area of functionality is degraded such that the business process cannot be delivered, and is affecting all Authorised Users.	2 hours	1 day
P3	Medium. Comprising: An important business function of the system is affecting a group of Authorised Users. Loss of an area of functionality impacting a group of Authorised Users. Performance of an area of functionality is degraded for a group of Authorised Users such that they are unable to deliver the business process.	4 hours	3 days
P4	Low. Comprising: Issue affecting a single Authorised User	24 hours	5 days
Service Request	For example: requests for information, advice and/or guidance.	None	None

## Annex: NEC Hearings Manager

Where NEC Hearings Manager 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 the General Provisions above, this Annex shall apply.

### Use of a third party's public cloud

Where stated in the Order Form, the Buyer consents to the use of a third party as a sub-processor of personal data for the purpose of providing cloud services, and acknowledges and agrees to the provision of those services on such third party's standard terms.

### Service Levels

All target times specified in the table below are measured within the Normal Support Hours.

Service Levels for NEC Hearings Manager			
Call Priority Level	Definition	Target Response Time	Target Resolution Time
P1	Critical. Comprising: The system is unavailable to all Authorised Users. Performance degraded to such an extent that NEC Hearings Manager is unable to be used by all users.	30 minutes	4 hours
P2	High. Comprising: Loss of a major area of functionality impacting all Authorised Users. Performance of a major area of functionality is degraded such that the business process cannot be delivered, and is affecting all Authorised Users.	2 hours	1 day
P3	Medium. Comprising: An important business function of the system is affecting a group of Authorised Users. Loss of an area of functionality impacting a group of Authorised Users. Performance of an area of functionality is degraded for a group of Authorised Users such that they are unable to deliver the business process.	4 hours	3 days
P4	Low. Comprising: Issue affecting a single Authorised User	24 hours	5 days

---

Service Request	For example: requests for information, advice and/or guidance.	None	None
-----------------	--	------	------

## Glossary

In addition to the terms defined elsewhere in this Agreement, the following terms (regardless of any other provision in this Agreement) shall have the meaning set out below:

“Additional Services”	means any support, maintenance and other services which are outside the scope of the Support Services and which Supplier has agreed to provide;
“Agreement”	means the Call-Off Contract;
“Authorised User(s)”	means those employees, agents and independent contractors of the Buyer who are authorised by the Supplier to use the SaaS and the Documentation;
“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;
“Business Day”	means any day which is not a Saturday, Sunday or bank or public holiday in England and Wales;
“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’s Support Team”	means those employees, agents and independent contractors of the Buyer who are authorised by the Supplier to use the Supplier’s support service;
“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;
“Call”	means notification of an Incident or Service Request by an Authorised User to the Service Desk in accordance with these Supplier Terms;
“Incident”	means any event which is not part of the standard operation of the SaaS and which causes, or may cause an interruption to, or a reduction in, the quality of that software or service;
“Normal Support Hours”	means Monday to Friday 09:00 to 17:00 (eight hours) UK time, each Business Day. For Stream, should the Particulars state that the Buyer has purchased 24x7 Support Services, Normal Support Hours shall mean 24x7x365/6 for P1 and P2 Incidents only and 09:00 to 17:00 (eight hours) UK time each Business Day for all other Incident Priority and Service Request calls;

---

“Particulars”	means the Order Form;
“Priority Level”	means the priority level of the Call reasonably specified by the Buyer’s Support Team, and agreed by the Supplier, according to the criteria set out in the applicable Annex;
“Problem”	means the unknown underlying root cause of one or more Incidents;
“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;
“Resolution”	means action which will resolve an Incident which may be a Workaround. “Resolve” and “Resolved” shall be construed accordingly;
“Response”	means contact via any means made by the Supplier to the Buyer’s Support Team or Authorised User in response to a Call reported via the Service Desk;
“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;
“Service Desk”	means the Supplier’s service desk detailed in these Supplier Terms;
“Service Level(s)”	means the service levels (as set out in these Supplier Terms) which apply in respect of the SaaS;
“Service Request”	means a Buyer’s Support Team request for information or advice and guidance;
“Supplier Support Team”	means the Supplier’s software support team which Resolves Calls;
“Support Services”	means the support and maintenance services which are provided by the Supplier as detailed in these Supplier Terms;
“Third Party Software”	means software which is proprietary to a party other than the Supplier and licensed to the Buyer by the Supplier;
“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; and

“Workaround”

means a method of avoiding an Incident or Problem either by a temporary fix or by a technique that means the Authorised User is not reliant on a particular aspect of the Supplier SaaS that is known to have an issue.

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

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