Transformation Partners in Health and Care
Digital Productivity

NHS

TPHC Digital Productivity Platform (DPP)

Supplier terms

RM1557.15 G-Cloud 15
v1 – January 2026

Contents

Supplier Standard Terms

Supplier Data Processing Agreement

Data Protection Protocol

Guidance: This Data Protection Protocol is for use alongside the proposed Call-Off Contract. The Table A at the beginning of the Protocol should be completed by the Buyer setting out the nature of the relationship and processing that will be taking place under the Call-Off Contract.

Table A – Processing, Personal Data and Data Subjects

This table A shall be completed by the Buyer, who may take account of the view of the Supplier, however the final decision as to the content of this table A shall be with the Buyer at its absolute discretion.

1. The contact details of the Buyer's Data Protection Officer are: [Insert Contact details]

2. The contact details of the Supplier's Data Protection Officer are: [Insert Contact details]

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that the Buyer is the Controller and the Supplier is the Processor for the purposes of the Data Protection Legislation in respect of: External applicants and internal applicants (ie employees) In respect of Personal Data where the Buyer is the Controller and the Supplier is the Processor, Clause 1 of this Protocol will apply.
Subject matter of the Processing	[Insert]
Duration of the Processing	[Insert]
Nature and purposes of the Processing	[Insert]
Type of Personal Data being Processed	[Insert]
Sensitive Data being Processed	[Insert]

Categories of Data Subject	[Insert]
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under union or member state law to preserve that type of data	[Insert]
Technical and organisational measures including technical and organisational measures to ensure the security of the data	*[The technical and organisational measures need to be described concretely and not in a generic manner.* *Description of the technical and organisational security measures implemented by the Processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the Processing, as well as the risks for the rights and freedoms of natural persons.* *Examples of possible measures (note that precise details must be given in relation to each measure – ie do not just repeat the high level bullet points below, as these are just examples of the types of measures):* • *Measures of pseudonymisation and encryption of Personal Data* • *Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services* • *Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident* • *Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the Processing* • *Measures for user identification and authorisation* • *Measures for the protection of data during transmission* • *Measures for the protection of data during storage* • *Measures for ensuring physical security of locations at which Personal Data are Processed* • *Measures for ensuring events logging*

	• *Measures for ensuring system configuration, including default configuration* • *Measures for internal IT and IT security governance and management* • *Measures for certification/assurance of processes and products* • *Measures for ensuring data minimisation* • *Measures for ensuring data quality* • *Measures for ensuring limited data retention* • *Measures for ensuring accountability* • *Measures for allowing data portability and ensuring erasure* *Description of the specific technical and organisational measures to be taken by the Processor to be able to provide assistance to the Controller.]*

Definitions

The definitions and interpretative provisions at Joint Schedule 1 (Definitions) of the Framework shall also apply to this Protocol. For example, the following terms are defined in Joint Schedule 1 of the Framework: "Buyer", "Data Protection Legislation", "UK GDPR", "Process" and "Processor" and "Supplier". Additionally, in this Protocol the following words shall have the following meanings unless the context requires otherwise:

"Controller"	shall have the same meaning as set out in the UK GDPR;
"**Data Protection Impact Assessment**"	means an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;
"**Data Protection Officer**"	shall have the same meaning as set out in the UK GDPR;
"**Data Recipient**"	means that Controller who receives the relevant Personal Data;
"**Data Subject**"	shall have the same meaning as set out in the UK GDPR;
"**Data Subject Request**"	means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
"**Data Transferor**"	means that Controller who transfers the relevant Personal Data;

"**Information Commissioner**"	means the Information Commissioner in the UK;
"**Joint Controllers**"	means where two or more Controllers jointly determine the purposes and means of Processing;
"**Personal Data Breach**"	shall have the same meaning as set out in the UK GDPR;
"**Processor**"	shall have the same meaning as set out in the UK GDPR;
"**Protocol**" or "**Data Protection Protocol**"	means this Data Protection Protocol;
"**Sensitive Data**"	shall mean the types of data set out in Article 9(1) or 10 of the UK GDPR;
"**Sub-processor**"	means any third Party appointed to Process Personal Data on behalf of that Processor related to this Call-Off Contract.

1. Supplier as data processor

1.1 Purpose and scope

1.1.1 The purpose of this Clause 0 is to ensure compliance with Article 28(3) and (4) of the UK GDPR.

1.1.2 This clause 1 applies to the processing of personal data as specified in table A.

1.1.3 Table A is an integral part of clause 1

1.1.4 This clause 1 is without prejudice to obligations to which the controller is subject by virtue of the UK GDPR

1.1.5 This clause 1 does not by itself ensure compliance with obligations related to international transfers in accordance with chapter V of the UK GDPR.

1.2 Invariability of Clause 0

1.2.1 The Parties undertake not to modify Clause 0, except for adding information to Table A or updating information in it.

1.2.2 This does not prevent the Parties from including the standard contractual clauses laid down in this Clause 0 in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict Clause 0 or detract from the fundamental rights or freedoms of Data Subjects.

1.3 Interpretation

1.3.1 Where this Clause 0 uses the terms defined in the UK GDPR, those terms shall have the same meaning as in the UK GDPR.

1.3.2 This Clause 0 shall be read and interpreted in the light of the provisions of the UK GDPR.

1.3.3 This Clause 0 shall not be interpreted in a way that runs counter to the rights and obligations provided for in the UK GDPR or in a way that prejudices the fundamental rights or freedoms of the Data Subjects.

1.4 **Hierarchy**

1.4.1 In the event of a contradiction between this Clause 0 and the provisions of the Call-Off Contract and/or related agreements between the Parties existing at the time when this Clause 0 is agreed or entered into thereafter, this Clause 0 shall prevail.

Description of the processing

1.4.2 The details of the Processing operations, in particular the categories of Personal Data and the purposes of Processing for which the Personal Data is Processed on behalf of the Controller, are specified in Table A.

1.5 **Obligations of the Parties**

1.5.1 Instructions

(i) The Processor shall Process Personal Data only on documented instructions from the Controller, unless required to do so by Law to which the Processor is subject. In this case, the Processor shall inform the Controller of that legal requirement before Processing, unless the Law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Controller throughout the duration of the Processing of Personal Data. These instructions shall always be documented.

(ii) The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe the UK GDPR.

1.5.2 Purpose Limitation

(i) The Processor shall Process the Personal Data only for the specific purpose(s) of the Processing, as set out in Table A, unless it receives further instructions from the Controller.

1.5.3 Duration of the Processing of Personal Data

(i) Processing by the Processor shall only take place for the duration specified in Table A.

1.5.4 Security of Processing

(i) The Processor shall at least implement the technical and organisational measures specified in Table A to ensure the security of the Personal Data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the risks involved for the Data Subjects.

(ii) The Processor shall grant access to the Personal Data undergoing Processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the Call-Off Contract. The Processor shall ensure that persons authorised to Process the Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

1.5.5 Sensitive Data

(i) If the Processing involves Sensitive Data as set out in Table A, or data relating to criminal convictions and offences, the Processor shall apply specific restrictions and/or additional safeguards as agreed between the Parties in Table A.

1.5.6 Documentation and compliance

(i) The Parties shall be able to demonstrate compliance with this Clause 0.

(ii) The Processor shall deal promptly and adequately with inquiries from the Controller about the Processing of data in accordance with this Clause 0.

(iii) The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations that are set out in this Clause 0 and stem directly from the UK GDPR. At the Controller's request, the Processor shall also permit and contribute to audits of the Processing activities covered by this Clause 0, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Controller may take into account relevant certifications held by the Processor.

(iv) The Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the

Processor and shall, where appropriate, be carried out with reasonable notice.

(v) The Parties shall make the information referred to in this Clause 0, including the results of any audits, available to the Information Commissioner on request.

1.5.7 Use of Sub-processors

(i) The Processor shall not subcontract any of its Processing operations performed on behalf of the Controller in accordance with this Clause 0 to a Sub-processor, without the Controller's prior specific written authorisation. The Processor shall submit the request for specific authorisation at least fourteen (14) days prior to the engagement of the Sub-processor in question, together with the information necessary to enable the Controller to decide on the authorisation.

(ii) Where the Processor engages a Sub-processor for carrying out specific Processing activities (on behalf of the Controller), it shall do so by way of a contract which imposes on the Sub-processor, in substance, the same data protection obligations as the ones imposed on the Processor in accordance with this Clause 0. The Processor shall ensure that the Sub-processor complies with the obligations to which the Processor is subject pursuant to this Clause 0 and to the UK GDPR.

(iii) At the Controller's request, the Processor shall provide a copy of such a Sub-processor agreement and any subsequent amendments to the Controller. To the extent necessary to protect business secret or other confidential information, including Personal Data, the Processor may redact the text of the agreement prior to sharing the copy.

(iv) The Processor shall remain fully responsible to the Controller for the performance of the Sub-processor's obligations in accordance with its contract with the Processor. The Processor shall notify the Controller of any failure by the Sub-processor to fulfil its contractual obligations.

(v) The Processor shall agree a third party beneficiary clause with the Sub-processor whereby - in the event the Processor has factually disappeared, ceased to exist in law or has become insolvent - the Controller shall have the right to terminate the Sub-processor contract and to instruct the Sub-processor to erase or return the Personal Data.

1.5.8 International Transfers

(i) Any transfer of data to a third country or an international organisation by the Processor shall be done only on the basis of documented instructions from the Controller or in order to fulfil a specific requirement under Law to which the Processor is subject and shall take place on the basis of an adequacy regulation (in accordance with Article 45 of the UK GDPR) or standard data protection clauses (in accordance with Article 46 of the UK GDPR). All transfers shall comply with Chapter V of the UK GDPR and any other applicable Data Protection Legislation.

(ii) The Controller agrees that where the Processor engages a Sub-processor in accordance with Clause 1.5.7. for carrying out specific Processing activities (on behalf of the Controller) and those Processing activities involve a transfer of Personal Data within the meaning of Chapter V of GDPR, the Processor and the Sub-processor can ensure compliance with Chapter V of the UK GDPR by using standard contractual clauses adopted by the Information Commissioner in accordance with Article 46(2) of the UK GDPR, provided the conditions for the use of those standard contractual clauses are met.

1.6 **Assistance to the Controller**

1.6.1 The Processor shall promptly notify the Controller if it receives a Data Subject Request. It shall not respond to the request itself, unless authorised to do so by the Controller.

1.6.2 The Processor shall assist the Controller in fulfilling its obligations to respond to Data Subject Requests to exercise their rights, taking into account the nature of the Processing. In fulfilling its obligations in accordance with Clauses 1.6.1 and **Error! Reference source not found.**, the Processor shall comply with the Controller's instructions.

1.6.3 In addition to the Processor's obligation to assist the Controller pursuant to Clause 1.6.2, the Processor shall furthermore assist the Controller in ensuring compliance with the following obligations, taking into account the nature of the data Processing and the information available to the Processor:

(i) the obligation to carry out a Data Protection Impact Assessment where a type of Processing is likely to result in a high risk to the rights and freedoms of natural persons;

(ii) the obligation to consult the Information Commissioner prior to Processing where a Data Protection Impact Assessment indicates that the Processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;

(iii) the obligation to ensure that Personal Data is accurate and up to date, by informing the Controller without delay if the Processor becomes aware that the Personal Data it is Processing is inaccurate or has become outdated; and

(iv) the obligations in Article 32 of the UK GDPR.

1.6.4 The Parties shall set out in Table A the appropriate technical and organisational measures by which the Processor is required to assist the Controller in the application of this Clause 1.6 as well as the scope and the extent of the assistance required.

1.7 **Notification of Personal Data Breach**

1.7.1 In the event of a Personal Data Breach, the Processor shall co-operate with and assist the Controller to comply with its obligations under Articles 33 and 34 of the UK GDPR, where applicable, taking into account the nature of Processing and the information available to the Processor.

1.7.2 <u>Personal Data Breach concerning data Processed by the Controller</u>

(i) In the event of a Personal Data Breach concerning data Processed by the Controller, the Processor shall assist the Controller:

(A) in notifying the Personal Data Breach to the Information Commissioner, without undue delay after the Controller has become aware of it, where relevant (unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(B) in obtaining the following information which, pursuant to Article 33(3) of the UK GDPR, shall be stated in the Controller's notification, and must at least include:

1) the nature of the Personal Data including where possible, the categories and

approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

2) the likely consequences of the Personal Data Breach; and

3) the measures taken or proposed to be taken by the Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(C) in complying, pursuant to Article 34 of the UK GDPR, with the obligation to communicate without undue delay the Personal Data Breach to the Data Subject, when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons.

1.7.3 Personal Data Breach concerning data Processed by the Processor

(i) In the event of a Personal Data Breach concerning data Processed by the Processor, the Processor shall notify the Controller without undue delay after the Processor having become aware of the breach. Such notification shall contain, at least:

(A) a description of the nature of the breach (including, where possible, the categories and approximate number of Data Subjects and data records concerned);

(B) the details of a contact point where more information concerning the Personal Data Breach can be obtained; and

(C) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(ii) The Parties shall set out in Table A all other elements to be provided by the Processor when assisting the Controller in the compliance with the Controller's obligations under Articles 33 and 34 of the UK GDPR.

1.8 **Non-compliance with Clause 0 and termination**

1.8.1 Without prejudice to any provisions of the UK GDPR, in the event that the Processor is in breach of its obligations under this Clause 0, the Controller may instruct the Processor to suspend the Processing of Personal Data until the latter complies with this Clause 0 or the Call-Off Contract is terminated. The Processor shall promptly inform the Controller in case it is unable to comply with this Clause 0 for whatever reason.

1.8.2 The Controller shall be entitled to terminate the Call-Off Contract insofar as it concerns Processing of Personal Data in accordance with this Clause 0 if:

(i) the Processing of Personal Data by the Processor has been suspended by the Controller pursuant to Clause 1.8.1 and if compliance with this Clause 0 is not restored within a reasonable time and in any event within one month following suspension;

(ii) the Processor is in substantial or persistent breach of this Clause 0 or its obligations under the UK GDPR;

(iii) the Processor fails to comply with a binding decision of a competent court or the Information Commissioner regarding its obligations pursuant to this Clause 0 or to the UK GDPR.

1.8.3 The Processor shall be entitled to terminate the Call-Off Contract insofar as it concerns Processing of Personal Data under this Clause 0 where, after having informed the Controller that its

instructions infringe applicable legal requirements in accordance with Clause 1.5.1(ii), the Controller insists on compliance with the instructions (provided that the Processor has clearly demonstrated the infringement by the provision of a legal opinion provided by a solicitor or barrister that both Parties can rely upon).

1.8.4 Following termination of the Call-Off Contract, the Processor shall, at the choice of the Controller, delete all Personal Data Processed on behalf of the Controller and certify to the Controller that it has done so, or, return all the Personal Data to the Controller and delete existing copies unless the Law requires storage of the Personal Data. Until the data is deleted or returned, the Processor shall continue to ensure compliance with this Clause 0.

2. Parties as joint controllers

2.1 Where in Table A the Parties acknowledge that, for the purposes of the Data Protection Legislation, the Buyer and the Supplier are Joint Controllers, this Clause 0 shall apply. The only Processing that a Joint Controller is authorised to do is listed in Table A of this Protocol by the Buyer and may not be determined by the Supplier.

2.2 The Parties shall, in accordance with Article 26 of the UK GDPR, enter into a Joint Controller agreement based on the terms outlined in Annex 1.

3. Both data controllers

3.1 To the extent that the nature of the Supplier's obligations under the Call-Off Contract means that the Parties are acting both as Controllers (as may be referred to in Table A), each Party undertakes to comply at all times with its obligations under the Data Protection Legislation and shall:

3.1.1 implement such measures and perform its obligations (as applicable) in compliance with the Data Protection Legislation; and

3.1.2 be responsible for determining its data security obligations taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects, and shall implement appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful Processing and accidental destruction or loss and ensure the protection of the rights of the Data Subject, in such a manner that Processing will meet the requirements of the Data Protection

Legislation where Personal Data has been transmitted by it, or while the Personal Data is in its possession or control.

3.2 Where Personal Data is shared between the Parties, each acting as Controller:

3.2.1 the Data Transferor warrants and undertakes to the Data Recipient that such Personal Data has been collected, Processed and transferred in accordance with the Data Protection Legislation and this Clause 0;

3.2.2 the Data Recipient will Process the Personal Data in accordance with the Data Protection Legislation and this Clause 0; and

3.2.3 where the Data Recipient is in breach of its obligations under this Protocol and the Data Protection Legislation, the Data Transferor may suspend the transfer of the Personal Data to the Data Recipient either on a temporary or permanent basis, depending on the nature of the breach.

Guidance: there are limited requirements in the UK GDPR when Parties act as separate Controllers. Clause 3 above provides a sensible starting point. However, Authorities are advised to review the Information Commissioner's guidance (ICO GDPR Guidance) and consultant their Information Governance team when considering whether further provisions or a separate data sharing agreement should be used.

4. Changes to this protocol

4.1 Any change or other variation to this Protocol shall only be binding once it has been agreed in writing and signed by an authorised representative of both Parties.

5. Joint Controller Agreement

In this Annex the Parties must outline each party's responsibilities for:

- *providing information to Data Subjects under Article 13 and 14 of the UK GDPR;*
- *responding to Data Subject Requests under Articles 15-22 of the UK GDPR;*
- *notifying the Information Commissioner (and Data Subjects) where necessary about Personal Data Breaches;*
- *maintaining records of Processing under Article 30 of the UK GDPR; and*
- *carrying out any required Data Protection Impact Assessment.*

The Joint Controller agreement must include a statement as to who is the point of contact for Data Subjects. The essence of this relationship shall be published.

Situations where both parties act as Joint Controllers are likely to be relatively novel. Therefore, in such circumstances, it will be important to seek specific legal advice on the approach to the Joint Controller agreement. As part of this, you may wish to include an additional clause apportioning liability between the Parties arising out of data protection in respect of data that is jointly controlled.

Annex 4 – Joint Controller Agreement

In this Annex the Parties must outline each party's responsibilities for:

- providing information to Data Subjects under Article 13 and 14 of the UK GDPR;
- responding to Data Subject Requests under Articles 15-22 of the UK GDPR;
- notifying the Information Commissioner (and Data Subjects) where necessary about Personal Data Breaches;
- maintaining records of Processing under Article 30 of the UK GDPR; and
- carrying out any required Data Protection Impact Assessment.

The Joint Controller agreement must include a statement as to who is the point of contact for Data Subjects. The essence of this relationship shall be published. Situations where both parties act as Joint Controllers are likely to be relatively novel. Therefore, in such circumstances, it will be important to seek specific legal advice on the approach to the Joint Controller agreement. As part of this, you may wish to include an additional clause apportioning liability between the Parties arising out of data protection in respect of data that is jointly controlled.

Supplier Service Specific Terms

Supplier SLA

Service Levels and Support Services

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings, and they shall supplement Schedule 4 (Definitions and Interpretations):

"Service Level Failure"	means a failure to meet the Service Level Performance Measure in respect of a Service Level;
"Service Level Performance Measure"	shall be as set out against the relevant Service Level in Part A of this Schedule;
"Service Level Threshold"	shall be as set out against the relevant Service Level in Part A of this Schedule;
“Support Services”	technical helpdesk services as set out in Part C of this schedule;

2. Service Levels

2.1 The Supplier shall use all reasonable endeavours to at all times provide the Services to meet or exceed the Service Level Performance Measure for each Service Level.

2.2 The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.

2.3 If a Service Level Failure occurs, the Supplier shall notify the Buyer in writing and shall, as soon as reasonably practicable, take all remedial action that is reasonable:

- to mitigate the impact on the Buyer;
- to rectify the Service Level Failure; and
- to prevent a further Service Level Failure from taking place or recurring.

3. Maintenance

3.1 The Supplier shall create and maintain a rolling schedule of planned maintenance to the Services (the “**Maintenance Schedule**”) which shall be shared with the Buyer.

3.2 The Supplier shall only undertake such planned maintenance (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule.

3.3 The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the Services.

3.4 Periods of Permitted Maintenance shall not count towards the calculation of the Supplier's performance against a Service Level Performance Measure.

4. Support Services

4.1 The Supplier shall provide the Support Services in accordance with Part C of this Schedule, in accordance with the timescales set out in Part C.

Part A – Service Levels

5. Service Levels

Service Levels			
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**
RaaS Service – Robot Accessibility	Accessibility rate of robots per month	99.998%	99.997%
Robot Processing Time	Time elapsed from the moment the request of the critical priority process is received/triggered until the process is started (excluding pending times).	<5 minutes in >99% of requests	>5 minutes for more than 1% of local transactions across the reporting period

Part B – Performance Monitoring

6. Performance Monitoring and Performance Review

6.1 The Supplier shall provide the Buyer with monthly performance monitoring reports ("**Performance Monitoring Reports**") which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

6.1.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;

6.1.2 a summary of all failures to achieve Service Levels that occurred during that Service Period; and

6.1.3 actions taken to resolve Service Level Failures and the action taken to remedy the underlying cause and prevent recurrence.

6.2 The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") on a monthly basis. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:

6.2.1 take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Buyer shall reasonably require;

6.2.2 be attended by the each Party's Contract Managers; and

6.2.3 be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer's Contract Manager and any other recipients agreed at the relevant meeting.

6.3 The minutes of the preceding month's Performance Review Meeting will be agreed and signed by both the Supplier's Representative and the Buyer's Representative at each meeting.

Part C – Helpdesk Technical Support Services

7. Roles and responsibilities

7.1 Supplier Responsibilities:

7.1.1 Management of the DPP Azure environment

7.1.2 Incident and support management

7.1.3 Capacity and performance management

7.1.4 Cloud access management and security control

7.1.5 Patching

7.1.6 Process build, change and configuration management

7.1.7 Performance monitoring and reporting.

7.2 Buyer Responsibilities:

7.2.1 Notifying of business application updates and downtime

7.2.2 Provision of test data and testing outcomes

7.2.3 Benefit reporting and KPI metrics

8. Service and support

Service Period	Tier	Assignment Group
Mon-Fri, 09.00-17.00*	T1	DPP PMO
Mon-Fri, 09.00-17.00*	T2	DPP Technical Team
Mon-Fri, 09.00-17.00*	T3	DPP Senior Team
Mon-Fri, 09.00-17.00*	T4	Solution Provider Escalation
*Excludes UK Public Holidays		

9. Service Categories

- **Incident Support -** Management of incidents and issue resolutions
- **Change Management -** Requests for changes to hosted processes in Managed Service and Hybrid Environments
- **Reporting Requests -** Requests for ad hoc reporting required outside of agreed monthly reporting schedules.
- **New Process Requests -** New developments into Managed Service and Hybrid Environments
- **Process Start/Stop**

10. Email Ticket Management

Service time	Initial response	Tier	Solution
Mon-Fri, 09.00-17.00*	60 minutes	T1	Convert to incident
Mon-Fri, 09.00-17.00*	60 minutes	T1	Convert to Service request
*Excludes UK Public Holidays			

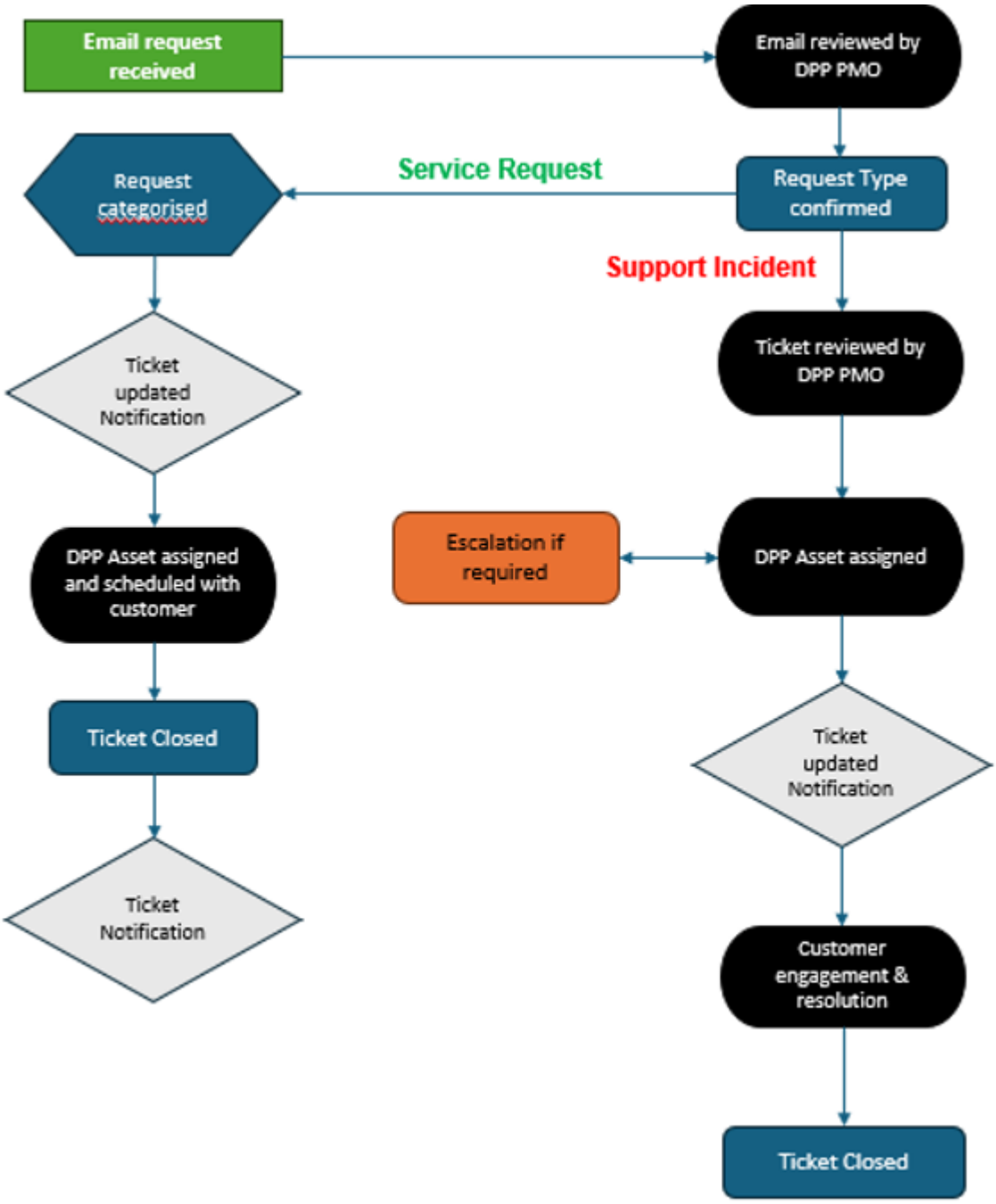
11. Service Requests

Request Category	Response	Solution or referral	Initial response level
Process change request	1 working day	Referral to T2	T1
New report	1 working day	4 hours referral to T2	T1
Report	2 hours	4 hours	T1
Scheduling change	2 hours	1 working day	T2
Onboarding new process	1 working day	Best efforts	T1
Start process	1 hour	2 hours	T2
Stop process	1 hour	2 hours	T2
General enquiry	1 working day	Best efforts	T1
Application downtime notifications	1 hour	4 hours	T2
*Excludes UK Public Holidays			

12. Incident Requests

	Tier 1 OLA			Group OLA
Service time	**Initial response**	**Tier**	**Solution or escalation**	**Response, solution, escalation**
Mon-Fri, 09.00-17.00*	30 minutes	T1	90 minutes	TBA
*Excludes UK Public Holidays				

13. Service Desk Management



Call-off Special Terms

Professional Services

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings, and they shall supplement Joint Schedule 1 (Definitions) RM1557.15:

"Professional Services"	means various digital productivity consultancy services provided by the Supplier as set out in a Statement of Work;
"Statement of Work"	means a detailed plan, agreed in accordance with Clause 1.4 below, describing the Professional Services to be provided by the Supplier, the timetable for their performance and the related matters.

1.2 The Parties shall agree a Statement of Work where the Buyer requires the provision of Professional Services under a Call-Off Contract.

1.3 The Supplier shall not undertake any Professional Services unless a Statement of Work is agreed in accordance with this Schedule and the Buyer shall not be liable to pay the Supplier for any Professional Services undertaken without such a Statement of Work being agreed for those Professional Services.

1.4 Each Statement of Work shall be agreed in the following manner:

1.4.1 the Buyer shall ask the Supplier to prepare a draft Statement of Work for Professional Services required by the Buyer;

1.4.2 within 3 Business Days of the Buyer's request, the Supplier shall notify the Buyer of any additional information it reasonably requires in order to prepare a Statement of Work;

1.4.3 within 3 Business Days of receipt of the required information from the Buyer, the Supplier shall provide the Buyer with the draft Statement of Work requested;

1.4.4 the Supplier and the Buyer shall discuss and agree that draft Statement of Work; and

1.4.5 both parties shall sign the draft Statement of Work when it is agreed.

1.5 Unless otherwise agreed, the price for Professional Services shall be calculated as set out in the Framework Prices.

1.6 Once a Statement of Work has been agreed and signed in accordance with clause 1.4 above, no amendment shall be made to it except in accordance with the Variation procedure.

1.7 Each Statement of Work shall be part of this Call-Off Contract and shall not form a separate contract to it.

1.8 Any Statement of Work still active at the time of expiry or earlier termination of this Call-Off Contract shall terminate immediately.