



Shared Business Services

Patient/Citizen Communication & Engagement Solutions Order Form (Service Level Agreement)

Framework details

Title: Patient/Citizen Communication & Engagement Solutions
 Reference: SBS10175
 Contract Duration: 1st November 2021
 Max End Date: 31st October 2025
 NHS SBS Contacts: Digital & IT Team mailbox
 Aidan Woodward (07395 253735) nsbs.digital@nhs.net
 Alison Pickup (07594 517789) aidan.woodward2@nhs.net
alison.pickup1@nhs.net

Order Form details

This Order Form is between the following parties and in accordance with the Terms and Conditions of the Framework Agreement.

Period of the Agreement	Effective Date	01 October 2025	Expiry Date	30 September 2027
-------------------------	----------------	-----------------	-------------	-------------------

Unless otherwise agreed by both parties, this Order Form will remain in force until the expiry date agreed above. The authority reserves the right to invoke a single 1 year (12 month) extension confirmed in writing no later than 1 month prior to the expiration date above. If no extension/renewal is agreed and the customer continues to access the supplier's services, the terms of this agreement shall apply on a rolling basis until the overarching Framework expiry date.

Supplier Order Form Signature panel

The "Supplier"	
Name of Supplier	Synertec Limited
Name of Supplier Authorised Signatory	[REDACTED]
Job Title of Supplier Authorised Signatory	Compliance & Commercial Support Manager
Address of Supplier	2 Chelston Business Park, Castle Road, Wellington, TA21 9JQ
Signature of Authorised Signatory	# [REDACTED]
Date of Signature	(dd/mm/yyyy) Full Name: [REDACTED]

Job Title/Role: Compliance & Commercial Support Manager

Customer Order Form Signature panel

The "Customer"	
Name of Customer	NHS England on behalf of South, Central and West Commissioning Support Unit.
Name of Customer Authorised Signatory	[REDACTED]
Job Title	[REDACTED]
Contact Details email	n/a
Contact Details phone	n/a
Address of Customer	Omega House, 112 Southampton Road, Eastleigh SO50 5PB
Signature of Customer Authorised Signatory	**** [REDACTED]

Date of Signature	(dd/mm/yyyy)

Authority Order Form Signature panel

The "Authority"	
Name of Authority	As Above
Name of Authority Authorised Signatory	As Above
Job Title	As Above
Contact Details email	As Above
Contact Details phone	As Above
Address of Authority	As Above
Signature of Authority Authorised Signatory	As Above
Date of Signature	As Above

This order form shall remain in force regardless of any change of organisational structure to the above named authority and shall be applicable to any successor organisations as agreed by both parties.

Table of Contents

1. Agreement Overview
2. Goals & Objectives
3. Stakeholders
4. Periodic Review
5. Service Requirements
 - a. Services Provided
 - b. Goods Provided
 - c. Price / Rates
 - d. Sub-contracting
 - e. Management Information
 - f. Invoicing
 - g. Cancellation
 - h. Complaints/Escalation Procedure
 - i. Termination
6. Other Requirements
 - a. Variation to Standard Specification
 - b. Other Specific Requirements

1. Agreement Overview

This Agreement represents an Order Form between *Synertec Ltd* and *NHS South Central and West CSU* for the provision of **Patient/Citizen Communication & Engagement Solutions**. This Agreement remains valid until superseded by a revised agreement mutually endorsed by both parties. This Agreement outlines the parameters for all **Patient/Citizen Communication & Engagement Solutions** covered as they are mutually understood by the primary stakeholders.

The Framework terms and conditions (including the specification of service) will apply in all instances, unless specifically agreed otherwise by both parties within this document.

2. Goals & Objectives

The **purpose** of this Agreement is to ensure that the proper elements and commitments are in place to provide consistent **Patient/Citizen Communication & Engagement Solutions** to the Customer by the Supplier. The **goal** of this Agreement is to obtain mutual agreement for **Patient/Citizen Communication & Engagement Solutions** provision between the Supplier and Customer.

The **objectives** of this Agreement are to:

- Provide clear reference to service ownership, accountability, roles and/or responsibilities.
- Present a clear, concise and measurable description of service provision to the customer.

3. Stakeholders

The primary stakeholders from the Supplier and the Customer will be responsible for the day-to-date management of the Agreement and the delivery of the service. If different from the Authorised Signatory details listed on page 1 of this Agreement, please provide the names of the **primary stakeholders** associated with this Order Form.

Supplier Contact: [REDACTED] – *Commercial Support Manager*

Customer Contact: [REDACTED] – *CHIS Associate Director, SCW CHIS*

4. Periodic Review

This Agreement is valid from the **Effective Date** outlined herein and is valid until the **Expiry Date** as agreed. This Agreement should be reviewed as a minimum once per financial year; however, in lieu of a review during any period specified, the current Agreement will remain in effect.

5. Service Requirements

A. Services Provided

Please detail the Lot(s) and Services that will be provided by the Supplier to the Customer

The Supplier will be providing services under Lot 6 of the Patient/Citizen Communication & Engagement Solutions (SBS10175) Framework.

B. Goods Provided

Please detail the goods to be provided or include an attachment with full details

Hybrid Mail and related communication services

The service must receive the letters electronically via the print function through our contracted system provider. The supplier will then be responsible for printing, enveloping, addressing and sending the letters. Provider IT infrastructure, Consumables (ink, envelopes, paper) and mailing will be included in the cost of the contract.

The supplier will be required to (amongst other things):

- Provide SCW CHIS the ability to view and update letter/message content.
- Print and address NHS branded letters and envelopes securely.
- Envelope letters securely.
- Dispatch letters within one working day securely, as per Letter Dispatch section below
- Send text messages via GOV.UK Notify, or other solution
- Capture delivery receipts.
- Send email messages via GOV.UK Notify, or other solution
- Generate and deliver reporting and management information
- Flex and vary the communication channels used to support the Government Digital Services' digital channel shift strategy in favour of digital communications.
- Continually develop the Hybrid Mailing capability to meet future requirements

Service Profile

Providing Printing and Mail and/or Digital patient communications from multiple Trust departments. Or any other service that the Supplier can provide that the Customer wishes to implement and utilise.

The Supplier will be providing the Customer with a hybrid mail and digital communications solution. The Supplier will be dealing with communications that are produced through the Trust's multiple administration systems and will print, collate, insert, and post correspondence on the resident's behalf, or communicate digitally depending on the Customers and individuals known preferences.

This will remove current costs associated with the printing of letter heads, letter printing, envelopes and franking.

Letter Dispatch

The Supplier will despatch same day as receipt from the Customer, and these will be sent out for delivery within 2 working days. Dispatch means that the letters have been printed at one of the Suppliers production sites and taken to Royal Mail via Whistl. The Supplier can only dispatch the same day if the letters are printed before 5pm. Delivery is then made by Royal mail within 2 working days as per our business class arrangement. The Customer can also use a first-class service which is a 1 working day turnaround for delivery

For documents being despatched on a 1st Class service

Documents received at a Supplier's Data Centre up to 17:00 would be expected to be printed, machine inserted and despatched the same day and handed over to Royal Mail for delivery to the recipient,

- It is expected that Royal Mail will deliver to the recipient on their next working day, e.g. Documents received and despatched on Monday should be delivered, by Royal Mail, to the recipient on Tuesday
 - Documents received and despatched on Friday should be delivered, by Royal Mail, to the recipient on Saturday

For documents being despatched on a Business Class service

Documents received at a Supplier's Data Centre up to 17:00 would be expected to be printed, machine inserted and despatched the same day to a Downstream Access provider and handed over to Royal Mail for delivery to the recipient,

- It is expected that Royal Mail will deliver to the recipient on their 2nd working day, e.g.:
 - Documents received and despatched on Monday should be delivered, by Royal Mail, to the recipient on Wednesday
 - Documents received and despatched on Friday should be delivered, by Royal Mail, to the recipient on Monday

Services will be provided in accordance with Schedule 5a – Framework specification;



Schedule 5a -
Framework Specifics

Key Performance Indicators (KPIs)

The following KPIs have been identified and will be measured in accordance with the standard rating system (Good, Approaching Target, Requires Improvement, Inadequate) set out within the Procurement Act 2023

- Enable SCW to have the ability to view and update letter/message content.
- Print and address NHS branded letters and envelopes securely.
- Deliver letters within two working days securely.
- Capture delivery receipts.
- Generate and deliver reporting and management information.
- Flex and vary the communication channels used to support the Government Digital Services' digital channel shift strategy in favour of digital communications e.g. text and email.
- Send text messages via Gov.UK Notify or other solution.
- Send e-mails via Gov.Uk Notify or other solution.

Social Value

The Supplier will be expected to work in collaboration with SCW to promote opportunities within the contract to deliver the following Policy Outcome and Model Award Criteria (MAC) as listed below:

- MAC 3.2 - Support innovation and disruptive technologies throughout the supply chain to deliver lower cost and/or higher quality goods and services.
- MAC 3.3 – Support the development of scalable and future -proofed new methods to modernise delivery and increase productivity
- MAC 4.2 – Influence staff, suppliers, customers and communities through the delivery of the contract to support environmental protection and improvement.
- MAC 8.2 – Influence staff, suppliers, customers and communities through the delivery of the contract to support strong, integrated communities.

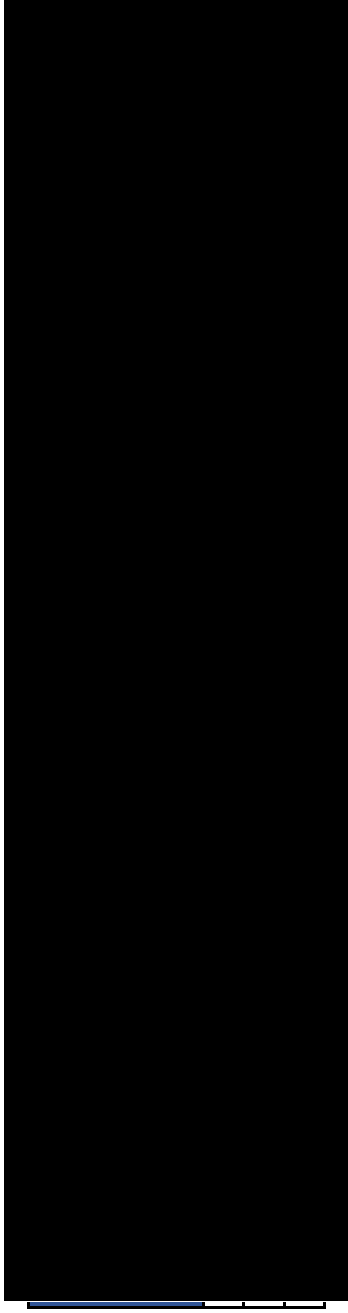
C. Price/Rates

Standard supplier pricing and rates are included within the pricing schedule. Please detail any discounts, volume arrangements or variations from the standard rates.

This is a Call Off Contract with a maximum Contract value of £6,644,145 Exc. VAT. The contract is based on a Call Off arrangement with no upfront commitment or minimum spend guarantee. Service charges will be made based on activity utilisation.

It is expected that VAT will be fully recoverable in accordance with the service as described within 'Contracted Out Services' under heading 61.

Estimated usage in relation to this contract is illustrated below;



SCW will only be charged for services consumed, with payment to be made bi-monthly following receipt of a valid invoice.

Charges for service will be based on the following price list.

Terms and Conditions

Pricing:

- 1. All prices quoted are exclusive of VAT
 - a. Syntec understands that the services it provides are compliant with the description of 'Contracted Out Services' under heading 61 of the HMRC VAT Guide Issued For NHS Bodies and are accepted and used as such by Trusts throughout the NHS to reclaim VAT
- 2. All prices are fixed for 30 days from the date of this document.
- 3. Printing and enclosing charges are calculated strictly based on the components used in the production of the document
 - a. See the tables above for further details on these components
 - b. Volume related discounts are applied to the component prices to calculate the total price charged
- 4. Any pre-printed material will be subject to an individual 'Additional Insert' charge
- 5. Postage is priced at Royal Mail Standard Account tariff, as existing from time-to-time
- 6. The Business Class Postal Discount and Economy Class Postal Discount will be given against the Royal Mail 2nd Class Standard Account tariff
- 7. The 1st Class Postal Discount will be given against the Royal Mail 1st Class Standard Account tariff
- 8. The following conditions apply to all postal discounts:
 - a. Envelope Size: C5
 - b. Envelope Weight: Less than 100 grams
 - c. Address Quality: Full and accurate address; matching the Royal Mail PAF database
 - d. Items which do not conform to the above requirements will not attract a discount and will be charged at Royal Mail Standard Account tariff
- 9. Where an organisation is using the Gov Notify service, SMS pricing shown is for creation only
- 10. Firetext SMS and Firetext Vanity Link pricing shown includes both creation and fragment charges
- 11. Syntec shall undertake an annual component price review, and where market conditions warrant, Syntec shall amend the Price List accordingly. Such price increases shall not exceed the CPI rate of inflation
 - a. For the avoidance of doubt the cost of processing and dispatching an average physical (PAYM) document shall be used in determining the price increase comparison to CPI, and this consist of:
 - i. 1 x C5 envelope
 - ii. 1 x white 80gsm paper
 - iii. 1 x duplex mono impression
 - iv. 1 x insertion charge
 - v. 1 x postage charge
 - vi. 1 x postage discount
 - b. Postage shall always be priced at Royal Mail Standard Account tariff, as existing from time-to-time and is not subject to the above CPI restriction

VAT will be recoverable as this service is compliant with the description of 'Contracted Out Services' under heading 61, (services of printing, copying, reproducing or mailing of any documents or publications, including typesetting services) in the HMRC VAT Guide Issued For NHS Bodies.

D. Sub-contracting

Subcontracting of services by Suppliers is allowed, both to Framework suppliers and to non-Framework suppliers. Any Supplier sub-contracting will be fully responsible for ensuring standards are maintained in line with the framework and this Order Form.

Synertec does not sub-contract any part of its service; other than the use of Royal Mail and other postal carriers for items mailed from its production centres.

E. Management Information (MI)

Suppliers should provide Management Information as standard on a monthly basis. Customers should detail any additional management information required and the frequency of provision here.

Management Information

Audit and Traceability

A full audit trail must be provided to replicate and enhance the information from the Customer's internal systems and provide full traceability and assurance that all documents have been processed as expected.

The Supplier will provide a comprehensive set of audit reports to ensure the Customer:

- Can confirm all of their documents have successfully reached Prism
- Have visibility of the document process, with each stage of this being transparent and easy to reconcile

Once the Customer's documents have reached Prism, the Supplier will ensure that the documents are processed as anticipated and despatched in expected timescales. However, the Supplier must stress that it is the Customer's responsibility to ensure that the correct number of documents have reached Prism, to help isolate any issues as soon as possible.

It is therefore essential that the Customer arranges for these reports to be viewed when received and any discrepancies highlighted as soon as possible to the Supplier, so they can be investigated and addressed accordingly. It is highly recommended that more than one person receives the reports, and that each report is received by an appropriate set of recipients to ensure document numbers are easily reconciled.

The Supplier must aim to meet their individual requirements with regards to audit and management information. Through control procedures the Supplier is able to track and trace each sheet of paper, each document, and each envelope all the way through production up to handover to the Royal Mail for final mile delivery. Final mile delivery refers to the final element of the delivery process – the postal staff physically delivering the letter to the recipient. Customer users have access to audit report information through the Prism Client desktop solution.

Typical information available includes:

- Quantity documents received
- Quantity documents printed and despatched
- Date documents received
- Date documents printed
- Date documents mailed
- Department where documents originated
- Number of enclosures
- Size of envelope i.e. C5, C4

The Supplier will manage the process of returned (undelivered) mail providing a service where returned mail is barcode scanned for identification. This allows the relevant packet details, along with the reason for the returned mail, to be sent to the Customer immediately in an electronic report. This allows the Customer to correct and resend documents to the intended recipients as quickly and efficiently as possible and improve the overall quality of their records. Once scanned, items are securely shredded on site.

The Supplier must provide a monthly management information report to detail total document and postal volumes for the Trust.

The Supplier must provide the facility for checking the Royal Mail PAF accuracy of a Customer's database of recipients to enable corrective measures to be taken, thereby maximising savings and minimising delivery delays for poorly constructed address records.
A report must be created and sent to the Customer to inform them which addresses failed to match the Royal Mail Postal Address File database.

F. Invoicing

Please detail any specific invoicing requirements here

For Printing, enclosing, envelope, postal and electronic charges, the Supplier shall issue invoices twice a month in arrears.

For monthly rental charges (relating to the Prism System), the Supplier shall invoice a month in advance.

The Customer shall pay the Supplier within thirty (30) days of the date of a Valid Invoice, submitted in accordance with this paragraph, the payment profile set out above and the provisions of the Contract.

The Supplier will invoice the Customer based on the Trust's usage during the billing period

In the event of any Party breaching a payment obligation, the other Party shall be entitled to charge interest on the outstanding amount in accordance with the Late Payment of Commercial Debts (Interest) Act 1998

Invoices are to be submitted per location, monthly in arrears based on services delivered.

Invoices are to be sent to the following address:

Odf Payables M425
PO BOX 312, LEEDS
LS11 1HP

Alternatively, electronic invoices are also accepted and can be submitted via Tradeshift. For more information please visit <https://www.sbs.nhs.uk/supplier-invoicing>.

Please note that Invoice must include the relevant Purchase Order Number.

G. Cancellations

Any variations to the standard cancellation terms detailed within the service specification should be captured here. Standard requirements from the specification are included for reference but may be amended to reflect local requirements.

n/a

H. Complaints/Escalation Procedure

Please detail any requirements regarding this

Points of Contact & Escalation**Customer Support**

Customers are assigned an office-based contact at all times. During implementation, this is the Project Support Advisor who will manage the process to successful completion. Once the service has been implemented, this is the Customer Services Advisor, who will be fully apprised of the customer's requirements.

The Customer Services Advisor is the day-to-day contact, and will be the dedicated contact point available to answer any questions or queries a Customer may have following implementation. They are responsible for:

- 'Logging' any issues reported, queries raised or changes requested by the customer on our internal support management system
- Ensuring that all 'logged' items are dealt with in a timely manner to SLA standards
- Ensuring appropriate customer contacts are kept informed as required
- Pro-actively managing customer production schedule requirements
- Escalating documents not received as expected
- Escalation Tree:
 - Customer Services Advisor
 - Customer Services and Support Manager – Public Sector
 - Customer Services and Sales Support Manager
 - Sales Director
 - Managing Director

The Customer Services Advisor will contact the Customer to introduce themselves and confirm their details. Each Advisor has a dedicated email address and direct dial phone number. In the event of absence, the Advisor's mailbox is monitored, and their phone number will divert to another member of the team.

Account Manager

Each customer will be assigned a field-based Account Manager who is responsible for the overall customer relationship. Account Managers are responsible for:

- Ensuring customers utilise our services to the maximum effect
- Ensuring service quality is of a consistently high standard
- Ensuring SLAs and KPIs are met
 - Conducting regular review meetings to discuss any areas of improvement /development of the service
 - Conducting regular review meetings to discuss any service issues including remedial actions
 - Conducting regular review meetings to discuss performance against SLAs and KPIs
 - Gathering detailed requirements for any new requests or significant changes to ensure that the customers' requirements are met
- Escalation Tree:

- Account Manager
- Regional Sales Manager – Public Sector
- Public Sector National Sales Manager
- Sales Director
- Managing Director

I. Termination

Standard requirements are provided below as an example but may be amended to reflect local requirements.

n/a

6. Other Requirements

A. Variation to Standard Specification

Please list any agreed variations to the specification of requirements

n/a

B. Other Specific Requirements

Please list any agreed other agreed requirements

Joint Schedule 11 (Processing Data)

Definitions

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

“Processor Personnel”	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;
------------------------------	---

Status of the Controller

2. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:
 - (a) “Controller” in respect of the other Party who is “Processor”;
 - (b) “Processor” in respect of the other Party who is “Controller”;
 - (c) “Joint Controller” with the other Party;
 - (d) “Independent Controller” of the Personal Data where the other Party is also “Controller”;

in respect of certain Personal Data under a Contract and shall specify in Annex 1 (*Processing Personal Data*) which scenario they think shall apply in each situation.

Where one Party is Controller and the other Party its Processor

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 (*Processing Personal Data*) by the Controller and may not otherwise be determined by the Processor.
4. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.
5. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:
 - (a) a systematic description of the envisaged Processing and the purpose of the Processing;
 - (b) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
 - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
 - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
 - (a) Process that Personal Data only in accordance with Annex 1 (*Processing Personal Data*) and shall not Process the Personal Data for any other purpose, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
 - (b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject. In the event of the Controller reasonably rejecting Protection Measures put in place by the Processor, the Processor must propose alternative Protective Measures to the satisfaction of the Controller. Failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures. Protective Measures must take account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Data Loss Event;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
 - (c) ensure that:
 - (i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*));
 - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

- (A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;
 - (B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
 - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
 - (D) have undergone adequate training in the use, care, protection and handling of Personal Data;
 - (d) not transfer, Process, or otherwise make available for Processing, Personal Data outside of the UK unless the prior written consent of the Controller has been obtained or the Controller has provided consent through Clause 13 (such consent may be withheld or subject to such conditions as the Customer considers fit at the Customer's absolute discretion) and the following conditions are fulfilled:
 - (i) the destination country has been recognised as adequate by the UK Government in accordance with Article 45 UK GDPR or section 74 of the DPA 2018;
 - (ii) Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 DPA 2018) as determined by the Controller;
 - (iii) the Data Subject has enforceable rights and effective legal remedies;
 - (iv) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
 - (v) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data;

if any of the mechanisms relied on under paragraph 6(d) in respect of any transfers of Personal Data by the Processor at any time ceases to be valid, the Processor shall, if possible, implement an alternative mechanism to ensure compliance with the Data Protection Legislation. If no alternative mechanism is available, the Controller and the Processor shall work together in good faith to determine the appropriate measures to be taken, taking into account any relevant guidance and accepted good industry practice. The Controller reserves the right to require the Processor to cease any affected transfers if no alternative mechanism to ensure compliance with Data Protection Legislation is reasonably available; and
 - (e) at the written direction, and absolute discretion, of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
7. Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to Processing Personal Data under or in connection with the Contract it:

- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
 - (b) receives a request to rectify, block or erase any Personal Data;
 - (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
 - (e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
 - (f) becomes aware of a Data Loss Event.
8. The Processor's obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
9. Taking into account the nature of the Processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
- (a) the Controller with full details and copies of the complaint, communication or request;
 - (b) such assistance as is requested by the Controller to enable the Controller to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
 - (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
 - (d) assistance as requested by the Controller following any Data Loss Event; and/or
 - (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.
10. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
- (a) the Controller determines that the Processing is not occasional;
 - (b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
 - (c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
11. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor once in any twelve (12) month period.
- (a) The Processor will allow the Controller or their nominated representatives to enter any premises where the Controllers Data is held, at all reasonable times and with prior notice, for the purpose of inspection providing such inspection would not (or there is no reasonable belief that it could) result in a breach of the Processors own security policies and procedures.

The Controller will take all reasonable measures to prevent unnecessary disruption to the Processors operations and will be responsible for all costs of carrying out such an audit

12. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

13. The Controller consents to the existing Subprocessors identified at the following



(a) Before allowing any new Subprocessor to Process any Personal Data related to the Contract, the Processor must:

- (i) Update the above location and notify the Controller in writing of the intended Subprocessor and Processing that will be undertaken by the Subprocessor;
- (ii) If the Controller does not consent to the new Subprocessor, they must communicate this in writing to the Processor within 30 days of being notified (such consent may be withheld or subject to such conditions as the Controller considers fit at the Controller's absolute discretion)
 - (A) If consent is not provided, then the Processor may not be able to deliver the services to the Controller. In this scenario, either Party shall be entitled to immediate terminate any agreement without liability or consequence ;
- (iii) enter into a written legally binding agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor, prior to any Personal Data being transferred to or accessed by the Subprocessor; and
- (iv) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

14. Any Processing by a Subprocessor or transfer of Personal Data to a Subprocessor permitted by the Controller shall not relieve the Processor from any of its liabilities, responsibilities and obligations to the Controller under this Joint Schedule 11, and the Processor shall remain fully liable for all acts or omissions of any of its Subprocessors. The exception to this is:

- (a) If the Controller sends Data to the Processor with the intention for it to be used to aid the Controller to integrate with another system or Processor, such as Gov.UK/Notify, then the Controller specifically authorises and instructs the Processor to transfer the data.
- (b) The Controller is responsible for ensuring that they have all necessary GDPR and data security arrangements for this onward processing of Data
- (c) The Processor shall not be liable or responsible for any damages or claims arising out of this transfer providing it has complied with the Controllers instructions and its obligations pursuant to this Data Processing Agreement

15. The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Where the Parties are Joint Controllers of Personal Data

17. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11.

Independent Controllers of Personal Data

18. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
19. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
20. Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
21. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
22. The Parties shall only provide Personal Data to each other:
 - (a) to the extent necessary to perform their respective obligations under the Contract;
 - (b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
 - (c) where it has recorded it in Annex 1 (*Processing Personal Data*).
23. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.
24. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

25. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract (**"Request Recipient"**):
 - (a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
 - (b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
 - (i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
 - (ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
26. Each Party shall promptly notify the other Party upon it becoming aware of any Data Loss Event relating to Personal Data provided by the other Party pursuant to the Contract and shall:
 - (a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Data Loss Event;
 - (b) implement any measures necessary to restore the security of any compromised Personal Data;
 - (c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
 - (d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
27. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 (*Processing Personal Data*).
28. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 (*Processing Personal Data*).
29. Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 18 to 28 of this Joint Schedule 11.

Annex 1

Data Processing Services

Processing, Personal Data and Data Subjects

1. The Provider must comply with any further written instructions with respect to processing by the Co-ordinating Commissioner.
2. Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Relevant Authority is the Controller and the Supplier is the Processor</p> <p>The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 of this Schedule 11 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ol style="list-style-type: none"> 1 Any Personal Data contained within the order/quote confirmation attachment provided to a Supplier for them to fulfil an order under the Call-Off Contract. 2 Any Personal Data for effective communication between the Authority and the Supplier. 3 Any Personal Data for maintaining full and accurate records of the Call-Off Contract. 4 Any Personal Data processed in the delivery of the services under the Call-Off Contract, including mailouts through postal or electronic communications and receipt of undeliverable communications. <p>The Parties are Independent Controllers</p> <p>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation and in accordance with Joint Schedule 11 in respect of:</p> <ul style="list-style-type: none"> • Business contact details of Supplier Personnel for the purposes of this Call-Off Contract • Business contact details of any directors, officers, employees, agents, consultants and contractors of the Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyers duties under the Contract for which the Buyer is the Controller.
Subject matter of the Processing	<p>The Supplier will be providing Printing and Mail and/or Digital patient communications from the Relevant Authority or any other service that the Supplier can provide that the Relevant Authority wishes to implement and utilise.</p> <p>The Supplier will be providing the Relevant Authority with a hybrid mail and digital communications solution. The Supplier will be dealing with communications that are produced through the Relevant Authority's multiple administration systems and will print, collate, insert, and post correspondence on the resident's behalf, or communicate digitally depending on the Customers and individuals known preferences.</p>

	<p>The service must receive the letters electronically via the print function through our contracted system provider. The supplier will then be responsible for printing, enveloping, addressing and sending the letters. Provider IT infrastructure, Consumables (ink, envelopes, paper) and mailing will be included in the cost of the contract.</p> <p>The supplier will be required to (amongst other things):</p> <ul style="list-style-type: none"> • Provide the ability to view and update letter/message content. • Print and address NHS branded letters and envelopes securely. • Envelope letters securely. • Dispatch letters securely (via Royal Mail) • Send text messages via GOV.UK Notify. • Capture delivery receipts. • Send email messages via GOV.UK Notify. • Generate and deliver reporting and management information
Duration of the Processing	Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract
Nature and purposes of the Processing	<p>Processing will include recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, analysis, restriction, erasure or destruction of data (whether or not by automated means).</p> <p>For the provision of a Hybrid Mailer solution where the supplier will be required to (amongst other things):</p> <ul style="list-style-type: none"> • Provide the ability to view and update letter/message content. • Print and address NHS branded letters and envelopes securely. • Envelope letters securely. • Dispatch letters • Send text messages via GOV.UK Notify. • Capture delivery receipts. • Send email messages via GOV.UK Notify. • Generate and deliver reporting and management information
Type of Personal Data	<p>Personal data Demographics including but not limited to name, date of birth, age, address, parents and carers</p> <p>Special Categories of Personal Data (health)</p> <p>Communications may contain Health Information pertaining to the Child Health Record including but not limited to:</p> <ul style="list-style-type: none"> • NHS • registered GP • birth details • childhood screening results • immunisation • progress reviews
Categories of Data Subject	<p>Staff (including volunteers, agents, and temporary workers)</p> <p>Customers/ clients, suppliers</p> <p>Parents / carers / family members</p> <p>Children aged 0-19</p>

International transfers and legal gateway	The Supplier will not transfer any Personal Data outside of the European Economic Area (EEA) without the prior written consent of the Authority
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	All relevant data to be deleted on expiry or termination of this Call-Off Contract unless longer retention is required by Law, as instructed by the Relevant Authority.