Macmillan Cancer Support

Invitation to Tender – Appendix 1- 4

Appendix 1

EVALUATION OF ADVANCED SPECIALIST PRACTITIONER

CARE HOMES PROJECT, BARNSLEY

July 2019

EXPRESSION OF INTEREST FORM	
Project title	Formative and summative evaluation of Macmillan's Advanced Specialist Palliative Care Practitioner project in Barnsley
Agency/Organisation name	
Agency/Organisation address	
Contact name	
Email address	
Telephone number	
Briefly indicate who you are proposing will carry out the evaluation and their relevant skills and experience (max 300 words).	
Briefly indicate the relevant previous evaluations undertaken by proposed team members. Projects cited should include dates and contract value (max 300 words).	

Appendix 2

FORM OF TENDER

DECLARATION

We do hereby offer to enter into a contract with the Macmillan Cancer Support on the terms and conditions of the Invitation to Tender, subject only to Tenderer Qualifications as may be agreed by the Macmillan Cancer Support.

We undertake to keep the tender open for acceptance by the Macmillan Cancer Support for a period of ninety (90) days from the return date.

We declare that this is a bona fide tender, intended to be competitive, and that we have not fixed or adjusted the amount of the tender by, or under, or in accordance with, any agreement or arrangement with any other person. We further declare that we have not done, and we undertake that we will not do, any of the following acts prior to award of this Contract:

    (a)   *Collude with any third party to fix the price of any number of tenders for this Contract;*

    (b)   *Offer, pay, or agree to pay any sum of money or consideration directly or indirectly to any person for doing, having done, or promising to be done, any act or thing of the sort described herein and above.*

We understand that you are not bound to accept the lowest price, or any, tender.

Signed:

Date:

Name:

in the capacity of:

duly authorised to sign tenders for and on behalf of:

Appendix 3

MACMILLAN QUALITY STANDARDS FOR EVALUATIONS

Theory of Change: Expectations of Development and Quality

Table 1 outlines a rubric with basic quality standards the Evaluation team uses when reviewing six elements of the Theory of Change process; analysis, participation/facilitation with programme stakeholders, causality, assumptions and the output.

In addition to the below, Macmillan encourages all bidders to refer to the Treasury's Green Book, Magenta Book and Aqua Book which provide useful guidance based on best practice in the field.

Table 1: Theory of Change Quality Standards Rubric

PRINCIPLES	WEAK	HAS POTENTIAL	REASONABLE	ROBUST
Comprehensive analysis	Superficial, uncritical, business as usual	Some new thinking, with big gaps in critical thinking	Critical thought on most areas, unclear in some areas, mainly based on known strategies	Critical, clear, focused, considers wide range of perspectives, information and strategies
Participation/Facilitation	Very few people involved ad hoc in formulation or review	Intentional inclusion of some players in formulation or review	Clear process for diverse input planned with wide participation in some aspects but not fully realised	Clear process implemented with critical input from diverse relevant players
Evidence-based/contextualised locally	Little to no elements of the theory of change (narrative, causal pathways, assumptions) supported by contextual evidence	Sporadic contextual evidence of elements of the theory of change	Critical elements of the theory of change with contextual evidence	All possible elements of theory of change comprehensively and systematically outline evidence in local context
Causality	No causal pathways made between individual components outlined in the theory	Some causal pathways between components made but not systematic or clear	Causal links of critical components of the theory of change have been made	Clear, comprehensive causal pathways for all components outlined in the theory of change

Articulated assumptions	None except most basic/obvious	Some but not systematic, clear or critical	Fairly complete but not all well formulated	Clear, comprehensive, critical ones identified
Output: Map and Narrative	Incoherent theory of change map with no accompanying narrative	A clear Theory of Change map but with little to no narrative	A clear Theory of Change map with critical pathways explained using change statements in accompanying narrative	Clear, comprehensive Theory of Change map with all causal pathways explained with change statements in accompanying narrative

Monitoring, Evaluation and Learning Framework: Expectations of Development and Quality

Table 2 outlines a Monitoring, Evaluation and Learning Framework template showing how the Evaluation team expects information included in a framework to be outlined. This does not represent the minimum information expected as part of a framework and should complement other information included as part of a framework.

Table 2: MEL Framework Template

Key Evaluation Question	Sub Question	Indicator	Target	Data Collection Method	Frequency	Responsible for Collection	Reporting
1.							
2.							

Table 3 provides a description of each framework element outlined with an expectation of standards of each element and example.

Table 3: Monitoring, Evaluation and Learning (MEL) Framework Element Standards

Framework Element	Description	Standard	Example
Key Evaluation Question	Key evaluation questions (KEQs) are the high-level questions that an evaluation is designed to answer and which determine what data to collect, how to analyse it, and how to report it.	The KEQs should be ideally defined in scoping the evaluation and should be developed with as many relevant stakeholders as possible who have an interest in the evaluation output.	Does the Macmillan Physical Activity Behaviour Change Care Pathway improve health and wellbeing for people with cancer?
Sub question	More specific questions which disaggregate a KEQ into constituent elements with clear reference to the variables whose measurement can help answer the KEQ – often between 1-5 evaluation sub-questions per KEQ.	These specific sub questions should be directly linked to the data collection tools.	Do people with cancer engage in more physical activity as a result of engaging with the programme?

Indicator	An outcome indicator provides a marker of whether a certain change has happened or whether certain conditions exist.	Each indicator should relate directly to one of the evaluation sub-questions – one or more indicator per sub-question. There should be a mix of quantitative and qualitative indicators, depending on the evaluation sub-questions and measures to which individual outcome indicators relate. An indicator should be; relevant and specific, consistent, credible, sensitive, unambiguous and feasible to collect.	Increase in time spent doing physical activity
Target	A target provides a standard or benchmark from which to judge the performance of the change that has been made. This allows the changes that have taken place to be judged in a systematic and transparent way and enables those analysing the data to determine whether, and in what ways, it has been a success or a failure.	When setting a target, these should be realistic and timebound. This should be agreed by those responsible for the performance of the programme and with understanding of the programme's capability and capacity. Targets should be informed using evidence-based benchmarks where possible.	5% increase in time spent doing physical activity from baseline
Data Collection Method	The data collection method is the mode/tool being used to gather the information required. Data collection methods can include a range of qualitative and quantitative methods such as; survey questionnaires, interviews, focus groups, observation, learning log, document review etc.	These methods should be selected based on how well they answer the key evaluation questions and with consideration of the programme resource available.	Survey Questionnaire (Scottish Physical Activity Questionnaire)
Frequency	Frequency should show the number of times or intervals the data outlined in the framework is to be collected.	This should be determined based upon how well this answers the key evaluation questions and with consideration of the programme resource available but should happen at a minimum before and after the intervention.	Baseline, and at 3, 6, 12 months.
Responsible for Data Collection	The individual/s gathering the data required for the evaluation as outlined in the	The person/s responsible for collecting the data should clear stated and identifiable	John Smith, Jane Smyth – Physical Activity

	framework.	with their name and roles stated.	Coordinators
Reporting	This shows when the data being collected is being used/shown in an output. This could include major evaluation outputs including interim and final reports as well as regular reports including monthly manager's update.	The outlined report outputs should be able to be recognised by all individuals involved in the evaluation.	Quarterly Performance Report Final Report

<div align="center">

Appendix 4

Information Security Assessment of 3rd Party Supplier

</div>

Introduction

This document is to assess the security credentials of a 3rd party supplier ("Supplier") before Macmillan enters into a data processor agreement.
The document should be completed by Macmillan information asset owner, the Supplier and Macmillan Security manager.
Macmillan may choose to audit the Supplier's response to this document.

Macmillan Asset Owner - Macmillan to Complete

This section should be completed by Macmillan information asset owner or delegate who plans to exchange information with a Supplier.

The name of Macmillan asset owner or delegate.	
The asset owner's Division or Function.	
A description of the information that will be exchanged with the Supplier.	
The classification given to the information. i.e. Restricted, Internal, Confidential or Public. (Should consider GDPR Sensitive Data)	
The date when the information will be exchanged.	
The period of time the information will exchanged.	
Mention why this Supplier was selected.	

Supplier Details- Supplier to Complete

This section should be completed by the Supplier.

The name and the role of the person completing this assessment.	
The company name of the Supplier.	
The service the Supplier intends to provide.	
Contact details for the Supplier.	
The date the Supplier completed this assessment.	

Supplier Security Assessment- Supplier to Complete

This section needs to be completed by the Supplier so that Macmillan is able gauge the Supplier's security position.

Where the Supplier does not have a security measure in place then a comment is required. If a measure is not applicable then just put in NA.

Item	Security Measures	Yes	No	Comments/Target Date
1	Compliance			
1.1	Is the Supplier registered with the Information Commissioner's Office under the Data Protection Act? If so provide registration number.			
1.2	Is the Supplier accredited to the ISO 27001 Security standard?			
1.3	Does the Supplier run yearly compulsory security awareness training to all staff including data protection and PCI DSS if applicable?			
1.4	Will the Supplier or its sub-contractors host Macmillan information outside the EEA?			
1.5	If the Supplier or it sub-contractors plan to take credit card payments on Macmillan's behalf are they PCI compliant? To what level?			
1.6	Does the Supplier have a responsible attitude to the Copyright, Designs and Patents Act (1988)?			
1.7	Will the Supplier remove all Macmillan data from their systems once the engagement is completed? Please explain how.			
2	Security Policy			
2.1	Does the Supplier have an information security policy which has been communicated to all their staff? Please send a copy.			
2.2	Does the Supplier review its security policy on yearly basis? Please state the date of the last review.			
2.3	Does the Supplier have a high-level infrastructure diagram and process flows for the service being provided? Please provide			
3	Organization and Information Security			
3.1	Does the Supplier have someone appointed in the role of Security Manager? Are staff aware of their information security responsibilities?			

3.2	Does the Supplier use a 3rd party supplier to host their information processing facilities and have they verified that the 3rd party has adequate information security measures in place? Are Macmillan's DP/ data security terms passed on to suppliers?			
4	Asset Management			
4.1	Does the Supplier clearly define information assets and assigned these to owners who are responsible for maintaining their protection?			
4.2	Does the Supplier have an information classification system to ensure that information receives the appropriate level of protection?			
5	Human Resource Security			
5.1	Does the Supplier put employees, contractors and sub-contractors through strict pre-employment vetting, including reference and security checks?			
5.2	Does the Supplier cover data protection and security in employment contracts?			
5.3	Does the Supplier ensure that employees, contractors and third parties exit the Supplier or change employment in an orderly manner?			
6	Physical and Environmental Security			
6.1	Does the Supplier implement security measures to prevent the unauthorised access to their premises, as well as, secure areas within their offices?			
6.2	Does the Supplier have measures to prevent the loss, damage or theft of equipment which may result in an interruption to the Supplier's activities?			
7	Communications and Operations Management			
7.1	Does the Supplier follow a formal IT service management process such as the IT Infrastructure Library (ITIL) to run its IT operations?			
7.2	Does the Supplier follow a formal change process to assess the impact of planned changes to its business?			
7.3	Does the Supplier employ network controls such firewalls and intrusion detection systems to protect their systems?			

7.4	Does the Supplier employ anti-virus software to protect computers and network gateways?			
7.5	Does the Supplier regularly patch computers on its estate to protect them against threats?			
7.6	Does the Supplier ensure that they use legitimate and correctly licensed software?			
7.7	Does the Supplier run a formal backup procedure to maintain the integrity and availability of their information processing facilities?			
7.8	Does the Supplier employ tools to exchange information with 3rd parties in a secure manner?			
7.9	Does the Supplier regularly perform Internet penetration tests on their network? How often? Please state when the last test was performed.			
8	Access Control			
8.1	Does the Supplier employ complex passwords for user accounts and require users to regularly change their passwords?			
8.2	Does the Supplier ensure that users only have access to the information they are authorised?			
8.3	Does the Supplier ensure that users cannot make unauthorized changes to computers or applications?			
8.4	Does the Supplier have a process to ensure that when people leave the organization their access to systems is disabled or removed?			
9	Information Systems Acquisitions, Development and Maintenance			
9.1	When the Supplier collects information on our behalf over the Internet are cryptographic controls employed to protect the collection of this information?			
9.2	Does the Supplier ensure that applications used to process Macmillan information do not introduce any errors or allow information to be misused, and the technology kept up to date?			

9.3	Does the Supplier develop their own web applications to collect and process Macmillan data and therefore make sure those applications are developed with information security in mind? eg. OWASP guidelines, ICO Privacy Impact Assessment guidance.			
10	Information Security Incident Management			
10.1	Does the Supplier have a defined process for managing information security incidents?			
10.2	Does the Supplier intend to report any information security incidents impacting Macmillan information immediately to Macmillan? How?			
11	Business Continuity Management			
11.1	Does the Supplier have a business continuity plan to protect the business from major failures and to ensure timely resumption? Disaster recovery? High availability?			
12	Cloud			
12.1	Does the Supplier maintain an active inventory of all cloud service connections in its environment?			
12.2	Are all cloud services connections tested and assessed?			
12.3	Does the Supplier control and monitor the use of cloud services by its staff?			
12.4	Are all cloud services connections secure?			

Macmillan Security Recommendation – Macmillan to Complete

This section is to be completed by Macmillan Security Manager once the sections above have been completed.

The name of the Security Manager	
The details of the security recommendation.	
The date the recommendation was completed.	
Should we proceed with this Supplier?	