# Application for Inclusion on an

# Open Select List

for

**Buildings Based Day Care Services**

**Document 6 of 6**

**November 2018**

**Expressions of Interest:** 06/11/18 to 14/12/18

**Submission Return Date: 14/12/18 at 5pm**

**This document is one of six parts as listed below, which together form the Invitation to Tender documentation. Please ensure that no part is missing or duplicated.**

|  |  |
| --- | --- |
| **Document No** | **Title** |
| Document 1 | Section 1: Information for ProvidersSection 2: Instructions to ApplicantsSection 3: Service Specification Section 4: Contract Management Schedule Section 5: Payment Schedule  |
| Document 2 | Section 6: Provider Responses – Open Select List Application  |
| Document 3 | Section 7: Payment DetailsSection 8: Declaration of Professional StandingSection 9: Form of TenderSection 10: Collusive Tendering CertificateSection 11: Freedom of Information Disclosure Form |
| Document 4 | Section 12: Provider Checklist |
| Document 5 | Section 13: Terms and Conditions of Contract |
| Document 6  | Appendix 1: Evaluation Matrix showing Quality CriteriaAppendix 2: Details for partners, consortium members or sub-contractorsAppendix 3: Meanings of OffencesAppendix 4: Minimum Information Security Standards And Acceptable Use |

# CONTENTS

**Section Description**

Appendix 1 Evaluation Matrix showing Quality Criteria

Appendix 2 Details for partners, consortium members or sub-contractors

Appendix 3 Meanings of Offences

Appendix 4 Minimum Information Security Standards and Acceptable Use

# APPENDIX ONE – EVALUATION MATRIX SHOWING QUALITY CRITERIA

# A copy of the Quality evaluation Matrix is shown below. Please note columns D to H of table 1 below are replicated for each supplier submitting a bid.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **D** | **E** | **F** | **G** | **H** |
|  |  | **Provider 1** |
| **Question Number** | **Methodology Statement** | **Evaluation panel scores** | **Average Score**  | **Weighted Score** |
| **1** | Please describe the Aims and Objectives for your Day Care service. |   |   |   |  |  |
| **2** | Please explain how you will involve customers and their carers in the Quality Assurance of the service to ensure services provided are of a high quality.  |   |   |   |  |  |
| **3** | Please describe how staffing and resources within your organisation will help to deliver the service outlined within the specification.  |   |   |   |  |  |
| **4** | Please explain how you will involve and communicate with service users to ensure their needs are being met on a day to day basis. |   |   |   |  |  |
| **5** | Please explain how you intend to adopt a person centred planning approach in order to deliver the service. Additionally, how you will ensure creativity and flexibility from your staff. Also, please describe the outcomes you envisage will be achieved.  |   |   |   |  |  |
| **6** | Please explain how due compliance with policies and procedures will enable you to provide high quality and positive experiences of a safe and effective service. |   |   |   |  |  |
|  |

*Table 1*

Each evaluator will score the responses to the Method Statement questions of each tender using the scoring scale detailed below and referred to in Section 1, paragraph 5.2.4:

|  |  |  |
| --- | --- | --- |
| **Score** | **Classification** | **Definition** |
| 0 | Unacceptable response (complete non-compliance) | No response at all, or insufficient information provided in the response, to the extent that proposal /submission is totally un-assessable and/or incomprehensible. |
| 1 | Unsatisfactory response (potential for some compliance, but one or more areas of major weakness). | Substantially unacceptable and weak submission which fails in several significant areas to set out a proposal that addresses and meets the requirements. Minimal, or little detail provided (and where evidence is required or necessary, no evidence or insufficient evidence provided) to support and demonstrate that the tenderer will be able to provide the service in question. Over-arching reservations regarding the tenderer's ability, understanding, expertise, skills and/or resources to deliver the requirements outlined. Would potentially represent a very high/high risk proposal for the contracting authority. |
| 2 | Satisfactory and acceptable response (substantial compliance with no major concerns) | Submission sets out a proposal which addresses and meets the requirements, with details and evidence provided to support the proposal. Some minor reservations or weakness in certain areas of the proposal in respect to relevant ability, understanding, expertise, skills and/or resources to deliver the requirements, but nothing that would prove detrimental to the level/ quality of service potential provided. Medium, acceptable risk solution to the contracting authority. |
| 3 | Good /very good response (fully compliant with all requirements, exceeding requirements in some instances) | Submission sets out a robust proposal that fully addresses and meets the requirements and in certain instances proposes additional value which exceeds the outlined requirements. Where evidence is required or necessary, full and relevant evidence had been provided to support the proposal. Provides full confidence as to the relevant ability, understanding, expertise, skills and/or resources to deliver the requirements. Low or no risk proposal for the contracting authority. |

*Table 2*

The average score for each question is then calculated by dividing the sum of the individual evaluator scores by the number of evaluators. For example, if there are 3 evaluators then the average score will be calculated as follows:

*(Evaluator 1 Score + Evaluator 2 Score + Evaluator 3 Score) / 3 = Average Score*

Following individual evaluation by each evaluator, a process of moderation is undertaken by the whole evaluation panel, the purpose being to gain consensus. This part of the process also ensures there is no significant variance between the scores of the individual evaluators. This process of moderation may result in individual evaluators revising their scores. Following the process of moderation the scores of the evaluation panel for the quality element of the evaluation will be finalised.

Any submission for the Experience and Method Statements section which achieves an overall score of less than 12 will entitle the Council, whose discretion in this matter shall be absolute, to reject. The score of 12 is equivalent to a score of at least 2 for each of the 6 questions in this section. In the scoring methodology to be applied, a score of 2 represents an acceptable response. The scoring matrix can be found in Table 2 above and also referred to in Document 1, Section 1, paragraph 5.2.4.

# APPENDIX TWO – DETAILS FOR PARTNERS, CONSORTIUM MEMBERS OR SUB-CONTRACTORS

STATEMENT OF NAMES AND PRIVATE ADDRESSES OF PARTNERS WITHIN THE PARTNERSHIP

DETAILS OF CONSORTIUM MEMBERS OR SUB-CONTRACTORS WHERE DELIVERING A SIGNIFICANT PROPORTION OF THE CONTRACT

|  |  |
| --- | --- |
| 1 | Name:(Private) Address: Post Code: |
| 2 | Name:(Private) Address: Post Code: |
| 3 | Name:(Private) Address: Post Code: |
| 4 | Name:(Private) Address: Post Code: |
| 5 | Name:(Private) Address: Post Code: |

PLEASE ADD FURTHER BOXES IF REQUIRED

# APPENDIX THREE – MEANINGS OF OFFENCES

**Glossary of meanings in relation to offences as described in Section 8 – Professional Standing**

Conspiracy - within the meaning of Section 1 of the Criminal Law Act 1977 (where that conspiracy relates to participation in a criminal organisation as defined in Article 2(1) of the Council Joint Action 98/733.JHA.

Corruption - within the meaning of Section 1 of the Public Bodies Corrupt Practices Act 1889, Section 1 of the Prevention of Corruption Act 1906; corruption as defined in Article 3 of the Council Act of 26 May 1997 and Article 3(1) of Council Joint Action 98.742/JHA.

Bribery as defined by the Bribery Act 2010

Fraud - where the offence relates to fraud affecting the financial interests of the European Communities as defined by Article 1 of the Convention relating to the protection of the financial interests of the European Union, within the meaning of:

Fraud or theft - within the meaning of the Theft Act 1968 and the Theft Act 1978

Fraudulent trading - within the meaning of Section 458 of the Companies Act 1985

Defrauding HM Revenue & Customs - within the meaning of the Customs & Excise Management Act 1979 and the Value Added Tax Act 1994

An offence in connection with taxation in the European community - within the meaning of section 71 of the Criminal Justice Act 1968

Destroying defacing or concealing of documents or procuring the extension of a valuable security - within the meaning of Section 20 of the Theft Act 1968

Money laundering - within the meaning of the Money Laundering Regulations 2003 and as defined in Article 1 of Council Directive 91.308.EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering

Any other offence - within the meaning of Article 45(1) of the Public Sector Directive

# APPENDIX FOUR – MINIMUM INFORMATION SECURITY STANDARDS AND ACCEPTABLE USE

**General**

Personal data shall be appropriately protected and only accessed for a lawful purpose at all times.

Personal data shall not be disclosed to any person or organisation unless authorised by LCC and as part of a written agreement e.g. information sharing agreement or written contract.

All staff involved in handling personal data shall complete locally arranged information security and data protection training.

Pre-employment checks that take into account relevant employment legislation including verification of identity are applied to all staff.

A security policy must be in place which sets out management commitment to information security and data protection and defines information security and data protection responsibilities.

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Any proposed transfers of personal data outside of the EU must be approved in advance by the data controller.

**Electronic Information**

Electronic copies of personal data supplied shall only be stored:

On hardware located in premises which are secure. This means premises which have suitable security measures to prevent. This means premises which have suitable security measures to prevent unauthorised access and to protect information and information assets. Security measures include control of access; locked windows and doors; intruder alarm; visitor control

On portable devices e.g. laptops, netbooks, which are encrypted using AES-256 bit encryption.

On removable media e.g. USB memory sticks, CD's, DVD's and external hard drives which are encrypted using AES-256 bit encryption

Electronic personal data shall not be transferred to any system not under the control of the third party e.g. a private laptop belonging to a staff member.

The use of unencrypted portable devices or removable media to store personal data shall not be authorised.

Portable devices and removable media shall be held under lock and key when not in use; data stored on removable media for the purpose of transporting data shall be securely deleted immediately after use e.g. USB sticks, external hard drives.

Access control (username & password) shall be in place across any device which is used to store electronic personal data.

Passwords shall consist of a minimum of eight characters including a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols.

Electronic copies of personal data shall be securely deleted when no longer required (in line with retention and disposal schedules). This includes data stored on servers, desktops, laptops or other hardware and media. Secure deletion means deleting files so they cannot be retrieved.

**Electronic Data Transfer**

Data transfer shall occur in the following ways; by secure email; by secure file transfer; via a trusted private network (utilised for the exchange of information without data traversing the public internet); or by secure courier services.

Secure email – personal data sent by email shall be transferred by attachment to an email between nominated GCSX, NHS.Net, PNN, GSI, GSX email accounts. Staff shall use the email addresses notified to the other party in advance of the data transfer to ensure that the recipient confirms successful receipt before data is sent.

Where GCSX email transfer is unavailable then an alternative secure email service shall be used e.g. LCC Secure mail. A secure email service is one which uses an encrypted communication/connection to deliver the email.

Secure Courier – data transfer shall be achieved using a signature service provided by a reputable secure courier. Removable media used to store the data shall be encrypted using AES 256 encryption. Passwords must be communicated separately and are not to be included with the media.

The receiving party must confirm by email that they are ready for the transfer and that the recipient address is correct before the transfer takes place. A further email must be sent confirming when the recipient has received, intact, the data.

**Network Security**

Personal data stored on a device/network which connects to the public internet shall implement the following controls which offer a sound foundation of basic security:

Boundary firewall and internet gateways: Information, applications and computers within the organisation’s internal networks should be protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.

Secure configuration: Computers and network devices should be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

User access control: User accounts, particularly those with special access privileges (e.g. administrative accounts) should be assigned only to authorised individuals, managed effectively and provide the minimum level of access to applications, computers and networks.

Malware protection: Computers that are exposed to the internet should be protected against malware infection through the use of malware protection software. Examples of Malware include viruses, worms, trojan horses, ransomware, spyware, and adware.

Patch Management: Software running on computers and network devices should be kept up-to-date and have the latest security patches installed.

**Hard Copy Information**

Hard copy personal data which includes printed material, files, and documents shall be stored under lock and key when not in use and access to the information shall be controlled.

Anonymised information shall be used wherever possible.

When printing off personal data only print the minimum necessary to achieve your aim.

When transporting hard copy personal data a locked briefcase or bag shall be used and it shall remain in your custody at all times. The personal information must not be visible through the bag.

Personal data shall only be removed from premises when absolutely necessary and shall be returned and locked away as soon as possible.

Hard copy personal data shall be destroyed securely when no longer required e.g. cross cut shredder. Alternatively it can be returned securely to LCC for destruction if local facilities are not available.

Data transfer of hard copy personal data shall be achieved by signature service recorded delivery or courier service in a sealed envelope, addressed to an individual by name or appointment.

**Security Incidents/Data Breaches**

The third party must notify LCC immediately of any information which has been subject to an actual or potential security incident or data breach including any failure to comply with the security requirement set out in this schedule.

The third party must fully co-operate with any investigation that LCC requires as a result of a potential security incident or data breach.

In the event of a security incident or data breach data transfers shall be delayed until the risk or issue is resolved.

If a security incident or data breach cannot be resolved following intervention data transfers shall stop unless the risk of stopping the transfer of personal data is outweighed by the need to transfer the personal data. Authority to continue must be provided by the information owner

**ACCEPTABLE USE**

**General**

In addition to the minimum security standards defined at Annex A individuals who utilise Lincolnshire County Council ICT assets, applications or services to process information must comply with the following standards:

You shall be responsible for your user name and password, access token or other mechanism as provided, and shall protect your user credentials against misuse.

You shall not use the user credentials of another person to access ICT, applications or services and you shall not share your own credentials with another person;

You shall only attempt to access ICT, applications or services that you have been given permission to access;

You shall not misuse the configuration or settings of any ICT;

You shall not attempt to bypass or subvert any security controls;

You shall not leave a computer system open if it is unattended.

You shall operate a clear screen policy when you leave ICT unattended, for example by “locking” the computer by pressing the Ctrl, Alt and Delete keys simultaneously and then click the “Lock Computer” button on-screen.

You shall not introduce unofficial software, hardware, removable media or files without appropriate authorisation.

**Unacceptable Use**

You shall not communicate information via an ICT system knowing it or suspecting it to be unacceptable within the context and purpose for which it is being communicated;

You shall not process or access racist, sexist, defamatory, offensive, illegal or otherwise inappropriate material;

You shall not carryout illegal, fraudulent or malicious activities;

You shall not store, process or displaying offensive or obscene material, such as pornography or hate literature;

You shall not break copyright.

**Monitoring**

Lincolnshire Council County reserves the right to monitor or record all Council communication systems including email, electronic messaging and internet use. Records of activity may be used by the organisation for the following purposes; Quality Assurance; conduct; discipline; performance; capability and/or criminal proceedings and any other purpose compliant with the regulatory and legislation framework in force and useful to support The Council's business activities

**Failing to Comply with the Minimum Standards**

Individuals who fail to comply with the minimum standards may have their access to Council assets, applications and services revoked and such action could have impacts on contracts with third party organisations and information sharing arrangements.