For Information

Part 2 Specification

Contract Reference

T00118CO

Contract Title

Customer Feedback Monitoring System

Contents

1. Overall Scope and Nature of the Requirement

The Council is looking to procure a new Customer Feedback Monitoring System, which must be in 'Live' use before 1st April 2019, with a period of parallel running with the current system prior to that date.

The system must be able to deal with Complaints/Compliments, Service Requests, Members' enquiries and MPs' enquiries. Optional requirements would be to log details of data breaches, FOI requests and SARs.

The system must be an established software solution and must be hosted by the Supplier. The maximum Budget for this Contract is £120,000. This is to include the initial set up cost and all annual fees, including Licensing, Support and Hosting for a maximum period of 5 years. Please refer to section 4.3 of Part 1 Information and Part 5 Pricing Schedule.

2. Mandatory Requirements

2.1 The Authority requires that the system must be:

(a) Fully developed;
(b) A web-based software application;
(c) Fully operational and currently used in a live environment;
(d) Hosted; and
(e) Kept fully functional with all supported versions of third party components, systems etc., for example databases, operating systems including mobile devices, report tools, browsers or any other products.

2.2 The system must be able to manage both Corporate and Children's Social Care complaints within the same database, using the same on-line form, so that cases can be common to the same customers and users (providing users have the relevant access permissions).

2.3 The System must have the functionality to enable members of the public to log their own complaints electronically.

2.4 As well as Complaints and Compliments, the System must be able to handle Service Requests and Member/MP Enquiries or at least be able to set up a separate reportable workflow to record these.

2.5 The cost of the 5 year Contract to run this system for the Authority must be £120,000 or less. This is to include the initial set up cost and all annual fees, including Licensing, Support and Hosting for a period of 5 years. **Please Note:** Where the Applicant's proposed submitted price exceeds this figure (the maximum total budget available), the Applicant will be deemed to have failed the process in its entirety and their bid will not be evaluated further.

2.6 The System must have the functionality to enable the Authority to set up customisable workflow processes as determined by its published complaints procedure and the statutory Children's Social Care complaints procedure including Local Government Ombudsman processes and Access to Information complaints processes. Also any other workflow processes, such as Member enquiries and service enquiries.

2.7 The System must have at least three tiers of users – basic user, departmental admin user and super user. Departmental admin users should only be able to control, manipulate and configure aspects of the system relating to their own department. Super users should be able to configure all aspects of the system, including setting up new users. There must also be a facility for external parties (e.g. arms-length organisations) to respond to cases allocated to them.

2.8 The System must have the functionality to format as output Email type messages for alerts to managers or other operational staff.

2.9 The system must be able to produce reports to enable comprehensive monitoring of performance both in terms of system generated reports and ad hoc reports created by users, including reports on learning from complaints and trends.

2.10 The System must contain a full audit of all activity and provide a management information reporting interface.

2.11 The system must be secure in the way it has been designed, developed and deployed and:

- It must contain parameters which can be set to enforce timeouts;
- It must have a password policy incorporating encryption, use of mixed case, numbers and special characters, minimum length, expiry, limit on login attempts, logging of unsuccessful login attempts and “forgotten password” functionality;
- Applicants must provide up-to-date documentation from the latest annual Application Penetration Testing undertaken by a reputable security vendor and provide evidence that any high priority items have been addressed. If this is not immediately available the Supplier must guarantee that this will be in place by the time the Contract is signed;
- Applicants must have general security procedures in place. These should include adherence to recognised standards (e.g. ISO/IEC 27001), equipment audits by a reputable third party (details of audits to made available on request);
- All personal data must be supplied using https (minimum level TLS 1.2);
- The Solution must ensure that all data is encrypted in transit; and
- The Solution must be capable of supporting a secure connection mechanism from the Authority’s network to the hosted System.
- Access to the Authority’s dataset must be limited to the Authority and approved personnel from the Supplier; and
- Applicants must have technical and procedural security measures in place to prevent:
  - Unauthorised or unlawful processing of personal data;
  - Accidental loss or destruction of or damage to personal data.

2.12 The system must be supplied with at least one environment in addition to the 'Live' environment, to be used for Testing and Training purposes.

2.13 The Solution must provide an availability level of 99.5% measured over a calendar month: twenty four (24) hours a day/seven (7) days a week.

2.14 Applicants must ensure that any enforced format or layout requirements imposed meet at least AA standards in terms of Accessibility (or give proof that they are working towards achieving AA standards).

2.15 The Authority's data must 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. The successful Applicant will be required to comply with the new General Data Protection Regulations when they come into force and any other changes in data protection legislation put in place post Brexit.

2.16 Applicants must ensure that the Solution is fully compliant with GDPR (General Data Protection Regulation).

2.17 Training must be available to support the implementation of the System.

2.18 Applicants must have appropriate Disaster Recovery / Business Continuity procedures in place (i.e. how the Organisation plans to ensure its continued functioning and servicing for this Contract, after a major event, e.g. a flood or fire that results in the loss of computers, telephones, premises etc.)

2.19 The Supplier must supply the Authority with all of its production data (in a format and time to be specified), with an appropriate database schema, free of charge at the end of the contract period.

2.20 The Applicant must ensure that the appropriate data is migrated from the Authority's current system in an accurate, correct and timely manner. Authority resources will be provided to extract data from the existing system.

2.21 The Authority must have full editorial capability over the style of the web pages and the content must fully adopt responsive web design.

2.22 Applicants must have a Service Level Agreement (SLA) for the hosting of the System. As a minimum the SLA needs to cover Back-Ups, System Restore, Integration with other systems, System availability/reliability, Service Credits, Turnaround time for Live to Test/Training environment refreshes (the Authority's requirement is within 2 working days), Turnaround time for changes in access rights to data or services (the Authority's requirement is within 2 working days), Loading of Software Patches and Upgrades (including Patches and Upgrades to Operating Systems and Third Party components), Details of where data back-ups will be held and what physical and electronic security will be used to secure them, equipment audits by a reputable third party (details of audits to be

made available on request) and reaction to information on potential security breaches;

2.23 The Authority must have free (of additional charge) access to its data for raw extraction. This can be supplied by any of the following:

2.23.1.1 By the Supplier providing full read access (not limited to standard working hours) to the authority's dataset for a limited number of individuals within the authority; or

2.23.1.2 Local replication; or

2.23.1.3 Remote replication to the Authority's site

2.24 The Supplier must supply the Authority with all of its production data (in a format and time to be specified), with an appropriate database schema, free of charge at the end of the contract period.

3. Specific Requirements

3.1 The system should enable customers to:

a) Log complaints and compliments
b) Follow the progress of their complaints.
c) Escalate a complaint if they are unhappy with the response they have received
d) Add contact details and their preferred method of communication.
e) Complete satisfaction surveys following a response to a complaint.

3.2 The system should enable Council Officers (including Admin) to:

a) Record premature Local Government Ombudsman complaints and automatically initiate the relevant complaint process.
b) Re-assign cases to another Council Officer, both en-masse, where an Officer is on holiday, sick leave or has left the authority, or on an individual basis.
c) Record that an external supplier should be included in any responses.
d) Record outcomes, lessons identified and recommendations made, and check that recommendations are implemented.
e) Record financial and non-financial settlements.
f) Personalise their use of the system, including the ability to edit correspondence templates, add shortcuts and customise screens and menus.
g) Discontinue a complaint, as the assigned officer.
h) Denote specific complaints as confidential, with access for specific users only.
i) View workload by Executive unit, department, team or assigned user.
j) Search for officer email addresses using Active Directory.
k) Create ad-hoc reports and create ad-hoc communication templates.

3.3 The system should:

a) Automatically generate customisable acknowledgements, responses and other correspondence relevant to the specific process being undertaken, either by email or hard copy print. The Authority must be able to edit all communications, prior to being sent.
b) Facilitate the uploading of attachments to cases.
c) Enable a complaint to bypass a particular stage of the complaints process.
d) Store additional information for Social Care complaints, for example investigating officers, Independent Person's, Panel Members, etc. and record money spent on these resources.
e) Link an assigned stage to relevant templates.
f) Prompt an officer to classify the issues raised by the customer so that the root cause of the complaint can be identified.
g) Capture Equalities information.
h) Facilitate an approval requirement for individual cases so that responses have to be checked before being sent out.
i) Enable a case to be assigned to several officers e.g. where a complaint is about multiple service areas

j) Store Reference numbers for the Complainant relating to other Council systems, for example Social Care, Council Tax and Housing Benefits.

3.4 Ideally the system should link to Active Directory for Single Sign On.

3.5 It would be useful if the system could also be used for all GDPR case types, FOIs, SARs and Data breaches so that all aspects of the Information Compliance team could be dealt with by one system.

3.6 The Applicant should provide the following information on how the System will be initially implemented and then supported during the term of the Contract with the Authority:

a) A clear overview of each component of the system (e.g. modules, Apps, etc.) and how it is licensed (e.g. site wide, named user, concurrent user) so the Authority knows exactly what it needs to purchase in order to meet the functionality required. Ideally to include an infrastructure diagram showing how the components are interconnected;

b) A high level implementation plan which describes how the System will be installed and deployed and a description of the tasks involved and resources needed. The Supplier will need to develop their outline plan into a full implementation plan on contract award.

c) Details of the system "Roadmap", i.e. a plan of future changes and enhancements, which should span at least 12 months in the future;

d) Details of the Service Level Agreement (SLA) for supplying comprehensive technical support for the system. The SLA needs to cover method(s) of incident reporting, incident categorisation, response times, methods of support, out of hours support, escalation processes, volume of use restrictions and any occasions where additional costs would be applicable;

e) Details as to the frequency of changes to the software (Releases/versions, and patches) as well as details of the circumstances in which new Releases will be charged for (if any). Also details on the extent to which previous and alternative versions of the system are supported and the level of control the Authority will have in terms of the timing of the installation of patches and new releases;

f) Confirmation that Client software application components (if any) provided as part of the solution are capable of unattended install;

g) A list of the mobile devices supported by the system;

h) Details of the policy for supporting new versions of Browsers as they are introduced, whilst still supporting older versions (with details of the browsers and versions currently supported by the system); and

i) Confirmation that system documentation is provided – as a minimum, this should be a user manual and a database schema, in hard copy or electronic format.

4. Contract and Performance Review Requirements

4.1 Contract and Performance Review Requirements

4.1.1 The Supplier must:

a) Provide a named contract manager;
b) Conduct regular contract review meetings at a frequency to be agreed post contract award;
c) In support of the contract review meetings, the Authority will require management meeting reports, the structure and format will be agreed at the first contract meeting.

4.2 Reporting Requirements

4.2.1 The Supplier must provide monthly reporting to cover the following:

a) Incidents – split by severity with the total number of incidents resolved within the SLA and those not resolved; and

b) Hosting– a list of all downtimes in the last month.

4.3 Service Credits

The Authority expects the Supplier to make provision for Service Credits where the service in respect of Support and Hosting does not meet specified levels.

Part 1: KEY PERFORMANCE INDICATORS (KPIs)

The KPIs which the Parties have agreed shall be used to measure the performance of the Services by the Supplier are contained in the below table.

4.3.1 System Availability

4.3.1.1 System availability will be measured as:

$$\frac{\text{Total minutes in month – planned downtime – unplanned downtime}}{\text{Total minutes in month – planned downtime}} \times 100\%$$

4.3.2 Some down time will be excluded from the calculation. This is as follows:

4.3.2.1 Planned downtime: is defined as:

a) where at least 10 working days notice of a system outage has been provided;

b) the impacts lasts for for less than 2 hours during the planned working day;

c) the impacts lasts for less than 10 hours overall;

d) there is at least a 3 month gap between planned occurrences. If less the outage will not be considered planned;

e) any downtime exceeding these parameters will be treated as included in the service level credit calculation.

4.3.2.2 Downtime not attributable to the hosting operation and is defined as:

a) any downtime where the problem is solely related to issues on the Authority's side regardless of how it was dealt with;

b) any down time associated with intermediate third party ISP's.

Exception: If a problem has been reported to the Supplier where the Supplier's early diagnoses suggests that the issue lies with the Authority but this is later proven to not be the case then this is NOT classed as Authority downtime. The start point of the down time will be from the moment the initial incident was recorded with the Supplier.

4.3.3 Incidents Performance

4.3.3.1 Different incident severity levels have their own corresponding Service level targets as follows:

4.3.3.2 **A. Critical**: 4 hour resolution (where the whole Live system is not available). This will be defined as not being met where either:

a) resolution takes longer than 4 hours; or

b) taking less than 4 hours but the whole Live system becomes unavailable again within one working day from time of resolution.

4.3.3.3 **B. Important**: 8 hours resolution (where a significant element of the Live system is not available). This will be defined as not being met where either:

c) resolution takes longer than 8 hours; or

d) taking less than 8 hours but a significant element of the Live system becomes unavailable within one working day of time of resolution.

4.3.3.3 **C. Minimal**: 40 hours (where no more than a few functions or a couple of users are unable to function)

4.3.3.4 **D. Minor**: on next release (all users are able to function).

4.3.4 The service level target is defined as:

The sum of:

The number of incidents recorded at severity level 1 multiplied by 8 (the weighting factor) +

Number of incidents recorded at severity level 2 multiplied by 6 (the weighting factor) +

Number of incidents recorded at severity level 3 multiplied by 4 (the weighting factor) +

Number of incidents recorded at severity level 4 multiplied by 0.5 (the weighting factor)

Incidents are only included in the measuring period in which they have been closed.

The Actual Service Level % is defined as above using only the incidents that have been resolved within the Service level resolution times, divided by the Service Level 100% Value.

Example:

Severity Level	Weighting	No. of Incidents	No. of incidents weighted	No. failed to meet SLA	No. met SLA	Met SLA weighted
1	8	3	24	0	3	24
2	6	6	36	2	4	24
3	2	9	18	0	9	18
4	0.5	18	9	0	18	9
Service Level 100% Value:			87	Actual Service Level Value:		75

In this example the Actual Service Level % = 75/87 = 86.21%

4.3.5 Helpdesk Response

4.3.5.1 To give an indication of how efficient the helpdesk is in the resolution of queries or calls.

4.3.5.2 Composition:

a) a baseline acknowledgment target would be set, e.g. 99% of calls should be acknowledged within 15 minutes of being logged for Critical and Important calls (as defined above).

b) at the end of every reporting period, the total number of calls registered on the helpdesk is analysed to determine volume of calls logged; percentage acknowledged within 15 minutes; average time taken in acknowledging the calls, total calls acknowledged; total calls acknowledged in 15 minutes and total time to answer.

4.3.6 Monitoring and Default

4.3.6.1 The Supplier shall monitor its performance against each Target KPI and shall send the Authority a report detailing Achieved KPIs in accordance with **Error! Reference source not found.**.

4.3.6.2 Where these KPI's are consistently not being met by the Supplier, i.e. 3 consecutive months in any rolling 12-month period, this would be considered a potential breach of Contract.

Part 2: SERVICE CREDITS

4.3.7 Calculation Of Service Credits

4.3.7.1 System Availability

4.3.7.2 Service Credits shall accrue for any reduction in availability over a calendar month (24/7) and shall be calculated in accordance with this Schedule.

4.3.7.3 If the supplier fails to meet the required availability level of 99.5% in a specific month, in terms of the functionality available to members of the public to enter feedback and the Authority to monitor, report on and respond to this feedback, they will be liable to give the Authority a credit against the Hosting fee charged for that month, as detailed in the table below:

Availability Level	% Service Credit Due
99.0 – 99.5%	5%
98.0 – 99.0%	15%
97.0 – 98.0%	25%
96.0 – 97.0%	35%
Below 96.0%	50%

Where the availability level falls below 90% this would be considered a potential breach of Contract.

4.3.8 Incidents performance

Service Credits shall accrue for any reduction in service levels over a calendar month (24/7) and shall be calculated in accordance with this Schedule.

If the supplier fails to meet the required service level in a specific month, in terms of the Service Level for each Severity Level of Incident, they will be liable to give the Authority a credit against the total admin fee charged for that month, as detailed in the table below:

Actual Service level %	% Service Credit Due
95.0 – 99.9%	5%
85.0 – 95.0%	15%

75.0 – 85.0%	25%
65.0 – 75.0%	35%
Below 65.0%	50%

Where the incidents performance level falls below 60% this would be considered a potential breach of Contract.

5 Invoicing

5.1 Payment Requirements

5.1.1 The Payment Schedule will be as follows:

a) Software Products – Perpetual Licence

- 50% on signature of the Contract;
- 25% on the expiry of the period set out in Acceptance Testing sign-off;
- 25% on implementation of the Software by the Authority in live mode.

OR

b) Software Products – SAAS (Software as a Service)

- 50% of first years' subscription on signature of the Contract;
- 50% of first years' subscription on implementation of the Software by the Authority in live mode;
- Software Subscription Charges shall be paid annually on the anniversary of the system go-live date.

c) Third Party Software (if appropriate)

- Full Payment on delivery

d) Hardware Products (if appropriate)

- Full Payment on delivery

e) Other Products (if appropriate)

- Full Payment on delivery

f) Implementation Services

- To be paid as days are taken, with 20% to be retained until the Software is in live mode.

g) Maintenance

- The first year's Charges will be paid from the system go-live date. Maintenance Charges shall be paid annually on the anniversary of the system go-live date.

h) Hosting

- The first year's Charges will be paid from the Date that any Torbay site is made available. Hosting Charges shall be paid annually on the anniversary of this date.

5.2 Invoicing

5.2.1 The Authority's settlement terms are 30 days from receipt of the goods and services or the invoice, whichever is the later.

5.2.2 The Contractor must always obtain an Authority official purchase order and quote the number on invoices.

5.2.3 Incorrect invoices will not be paid and a corrected invoice will be requested.

5.2.4 Payment will be by BACS and remittance advices will be transmitted to the Contractor by email or fax if email addresses and/or fax numbers are provided.

6 Added Value

6.1 Further Services Offered

The Applicant will be expected to suggest as part of its response to the Evaluation Questions any additional products or services that they may be able to offer as part of this Contract or any other added value that their offer might be able to bring to the Authority. Applicants are expected to build any such offers into their submissions regardless of whether specific questions are asked along these lines or not.

7 Awarding the Contract on Behalf of Other Contracting Authorities

7.1 The Authority is not purchasing on behalf of other contracting authorities.

But this Contract will be used by the Authority's agents and arms-length organisations, e.g. TOR2, Torbay Development Agency, The English Riviera Tourist Board, and any future arms-length organisations.