personal info

Shropshire
Council

10 October 2016

RMCI 019

Please ask for: [redacted]

Email: **procurement@shropshire.gov.uk**

Dear Tenderer,

RMCI 019- SUPPLY OF SOCIAL CARE SYSTEM

TENDERED UNDER CCS FRAMEWORK RM1059 LOT 6

SHROPSHIRE COUNCIL

You have been invited to tender for the above requirement. With this letter please find enclosed a copy of the following documentation: -

Invitation to Tender including;

- Instructions for tendering
- Requirements Specification (Appendix 1)
- Tender Response (Appendix 1)
- Pricing Schedule (Appendix 1)

Tenders should be made using the enclosed Invitation to Tender including Appendix 1. Your Tender must be completed, signed and returned together with a signed copy of the 'Instructions for Tendering' through our Delta Tenderbox. You are recommended to keep a copy of all tender documents and supporting documents for your own records.

PLEASE INFORM THE COUNCIL AS TO WHETHER YOUR ORGANISATION IS GOING TO TENDER AND LET THE COUNCIL KNOW BY **OCTOBER 14 2016** through the Delta Portal

Please note the reference to Telford and Wrekin Council in Appendix 3.

Returning of Tenders

The deadline for returning tenders is **NOON ON NOVEMBER 11 2016**, any tenders received after this time will not be accepted.

Tenders are to be submitted through Delta, our electronic tender portal.

- Please ensure that you allow yourself at least two hours when responding prior to the closing date and time, especially if you have been asked to upload documents. If you are uploading multiple documents, you will have to individually load one document at a time or you can opt to zip all documents in an application like WinZip. Failure to submit by the time and date or by the method requested will not be accepted.

- **Once you upload documentation ensure you follow through to stage three and click the 'response submit' button. Failure to do so, will mean the documents won't be viewable by the Council.**

Tenders must be made using Delta and **cannot** be accepted if:

- They are received by post, facsimilie or email
- They are received after **12 noon on the given deadline**

Freedom of Information

Under the provisions of the Freedom of Information Act 2000 from 1 January 2005, the public (included in this are private companies, journalists, etc.) have a general right of access to information held by public authorities. Information about your organisation, which Shropshire Council may receive from you may be subject to disclosure, in response to a request, unless one of the various statutory exemptions applies.

Therefore, if you provide any information to Shropshire Council in the expectation that it will be held in confidence, you must make it clear in your documentation as to the information to which you consider a duty of confidentiality applies. The use of blanket protective markings such as “commercial in confidence” will no longer be appropriate and a clear indication as to what material is to be considered confidential and why should be given.

Other Details

Please note that if supplementary questions are raised by any tenderer prior to the closing of tenders and Shropshire Council decides that the answers help to explain or clarify the information given in the Tender Documents, then both the questions and the answers will be circulated to all enterprises invited to submit a tender.

If you have any queries relating to this invitation to tender, please contact me through the Delta Portal.

Yours faithfully

[redacted]

Commissioning Development & Procurement Manager

Commissioning Development & Procurement

procurement@shropshire.gov.uk

Enc

Shropshire Council

Invitation to Tender

RMCI 019

Integrated Adults and Children's Social Care Case Management and Finance System

Further competition through Crown Commercial Services (CCS) Framework – RM 1059 – Lot 6 Social Care

Table of Contents

Appendices

1.0) Introduction

1.1 General Requirements

Tenders are invited for the provision and maintenance of an integrated Social Care Case Management and Financial solution for Adults and Children's Services. The system needs to support current and future end-to-end business processes enabling the Council to introduce a more integrated holistic or 'whole-family' approach to service delivery, which involves partners and providers and can support child to adult transition, mobile working, service demand forecasting and resource planning and allocation.

This procurement is to be run as a further competition under the CCS Framework RM 1059 'Local Authority Software Applications' Lot 6-Social Care Systems.

The Council's complete requirements and the pricing response document are as detailed in Specification of Requirements and Tender Response document in Appendix 1.

1.2 Background

The Council has established a project to replace the current Adults and Children's Social Care Business system as part of a Digital Transformation Programme. The system will replace the current OLM CareFirst Social Care system, which was purchased over 10 years ago and our current implementation no longer meets all of our social care system requirements.

The Council requires a social care case management solution, including an integrated financial solution to be ready for implementation by April 1 2018.

The system is to be hosted by the successful supplier working in partnership with Council staff responsible for service delivery.

The system needs to be an integrated ICT solution for both Adults and Children's social care that incorporates contract management, financial processes, electronic document management and fully integrated workflow and supports the operational, tactical and strategic management of social care services. The system should facilitate risk management, service contract management, financial budgetary management and the management of a case from assessment to the delivery and payment of care services.

1.3 Key Business Objectives of Procurement

The key objective of the procurement exercise is to implement an information system that supports all social care functions of Shropshire Council and relevant partner agencies enabling the Council to improve its service offering to citizens and ultimately to ensure that the social care needs of adults and children are met. This will be achieved through the procurement of a solution that:

- Enables the Council to easily and accurately analyse and forecast demand for services
- Enables the Council to easily and responsively understand resources, requirements, capabilities and costs
- Supports managers to plan services effectively and to allocate appropriate resources
- Optimises the use of available modern technologies such as online portals, SMS, email, customer insight analysis tools and social media to improve communications and operational interactions with citizens, partners and providers
- Allows the Council to effectively control all financial elements related to the delivery of social care
- Supports the Council's adherence to relevant national and local strategies, policy directives and statistical returns
- Facilitates multi-agency working and service delivery
- Provides standard and customisable management information to support service delivery planning, monitoring and outcome measurements

- Supports the operational business processes employed by the Council including workflows and event chronology
- Provides a secure and stable environment for the storage and retrieval of data
- Eases data input and access through intelligent/logical questioning and prompts, tips and real-time error messaging

The system will generate payments to providers and charges to individuals in line with Council policy and the system will be able to provide the necessary requirements for Care Accounts for adult citizens.

It will be flexible, easy to use, intuitive and capable of being integrated with core Council systems, where appropriate. It will also be accessible securely by Council staff, and by their public and private sector partners, using web based technology to support case reviews and to develop and maintain action plans.

Our objectives include:

- To fully implement an integrated solution for both adults and children's social care and financial management system by April 2018.
- Deliver a solution that is universally recognised by staff as being a significant improvement on existing arrangements.
- Deliver a solution that fully exploits modern technologies and supports joined up, anytime, anywhere working.

A single view of service users and their relationships is a key strategic goal for the solution which should support:

- The requirement to manage a case from assessment to delivery of a care service, including costs and payments and also keep a record of children and vulnerable adults who are not currently receiving services from us but who we are aware of.
- The requirement for different services / teams to be able to interface with the same record on an open case.
- The requirement for relevant Council staff and partner agencies to have access to an electronic case file to support case reviews and to develop and maintain action plans.
- The requirement to link systems together to enable the flow and connectivity of data in order to share intelligence and minimise manual data inputting.
- The recording of financial information against both individuals and contracts.
- Integration with NHS systems.

1.4 Scope of The System

The scope of the system and the response to the tender is as detailed in the Specification of Requirements and Tender Response document - Appendix 1. However, if the Tenderer has a facility which would genuinely add value to the solution and is totally relevant then it may outline the detail, benefits and cost of the facility accordingly against the Value Added Question of each tab in the Specification of Requirements.

The overall solution must enable the Council to carry out its Social Care responsibilities within Adults and Children's Services in line with government requirements around the Care Act and increased partnership working across agencies.

The system must enable the Council to meet all relevant legislation and security requirements to keep records and information safe and secure, in particular to integrate with NHS systems. It must be seen as assisting and not delaying or hindering social workers and other users. The system is required to support the Council in monitoring and evaluating the work to be done and therefore reporting and data management functionality is essential.

1.5 Peripheral Systems

Current IT Systems in use across Social Care

CareFirst is used to administer and manage both Adults and Children's Social Care Records in Shropshire and is linked to the Electronic Document and Records Management System CareStore.
A number of other IT systems are in use across the Council which interact (directly and/or indirectly) with CareFirst to enable the Council to undertake its tasks in relation to Social Care and these are outlined below:

CASPAR

Purpose

- Client Money and Case Management System for Appointees and Public Authorities Deputies

Functionality

- Recording of planned income and expenditure transactions for clients
- On-screen bank account reconciliation
- Integration to online banking systems
- Court of Protection workflow and forms
- Deputyship Form production
- Appointee and Deputy Fee Management
- Property and Personal Effects registers

CM2000 Call Confirm

Purpose

- Scheduling system for Care Workers and electronic call monitoring

Functionality

- Auto create visit schedules
- Send schedules and updates to workers via mobile phone
- 'Match' unallocated visits to most suitable Care Worker
- Manage absences
- Produce payroll export
- Real time logging of calls made and duration
- Monitoring of care providers service delivery

CM2000 Finance Manager

Purpose

- Automate and manage provider payments

Functionality

- Import purchase order information from case management system
- Match purchase order information to Care Providers visit data
- Reconcile, arbitrate and authorise invoice totals
- Export invoice information to case management system for payment

Civica Icon

Purpose

- Used by Financial Assessment Team as electronic client file and workflow tool

Functionality

- Store electronic documents against clients
- Attach processes/workflow to clients
- Generate actions to team members to appear in In-Tray
- Access Revenue and Benefits information to confirm/cross check financial information

CHARMS

Purpose

- Adoption Case Management for Joint Adoption Service

Functionality

- Create record at Family level, containing separate individual's information within the Family record
- Create child record
- Record assessment stages and approvals
- Generate potential matches between children and families
- Record placements of children with families

E-CINS

Purpose

- Strengthening Families and Early Help case management

Functionality

- Maintain case record with Assessments and Action Plans
- Share information securely across multiple agencies
- Automated notifications and updates to users
- Provide Troubled Families outcomes data
- Provide Early Help data

Open Objects

Purpose

- Used by Family Information Service to meet statutory requirement under the Child Care Act to provide information to Parents and Carers via the Internet

Functionality

- Extended Child Care Directory (ECD) – import from Capita ONE of Ofsted registered Child Care providers
- Family Services Directory (FSD) – manual input of information

E-Start

Purpose

- Used by Children's Centre Services Team to manage and monitor the service usage in term of service planning, forecasting, Ofsted inspections etc.

Functionality

- Create record at family level with unique number
- Associate individual family members to the family, each individual has unique number
- Record family registration form
- Record activity of family attendance at groups and activities
- Record support provided to partner groups
- Reporting function

Capita ONE

Purpose

- Education Management System used by the Authority

Functionality (used by Social Care):

- Recording of Children with Disability
- Children/families registered with All In (Short Break provision)
- Attendance at All In (Short Break provision)
- Record enquiries to Family Information Service

Microsoft Dynamics

Purpose

- CRM for all initial contacts with Council for either Adults or Children

Functionality

- Create record of person
- Record reasons for contact and outcome
- View history of contacts
- Built in workflow to determine route for contact

1.6 Pricing – Specification of Requirements

Where the Council is looking to replace, integrate or interface to the functionality of the systems detailed in 1.5 Peripheral Systems, then this is included in the relevant sections of the Specification of Requirements and Tender Response document – Appendix 1. In this document Tenderers are invited to explain how their solution will meet the needs of the Council in respect of 'peripheral systems', including how the proposed solution either includes/integrates the functionality of such systems or how the solution might interface to a third party system. Tenderers are expected to have priced those integrations, modules and interfaces to third parties within the price of their overall system solution – hereafter referred to as the 'Whole Life Costs'.

The Council understands that the solutions proposed by tenderers in respect of peripheral system functionality could be quite varied and could include different combinations of an integrated, modular or interface approach. To that end, tenderers are asked to do the following:

a) Provide a Whole Life Cost, which includes all of the functionality outlined throughout the requirements specification that the tenderer is able to supply including peripheral system functionality i.e.:

- Interface to CRM
- Interface to Corporate Finance Systems
- Children's Centres Solution/Interface
- Strengthening Families and Early Help Case Management Solution/Interface
- Family Service Directory Solution/Interface
- Mobile Working Solution
- e-Marketplace
- Online Secure Portal Facility
- Diary Management Solution/Interface
- Adoption Case Management Solution/Interface
- Solution or Interface to Administer Client Money for Appointees and Public Authorities Deputies
- Workforce Management - Rostering/Scheduling/Care Monitoring Solution/Interface
- Provider Payments Solution/Interface
- Financial Assessments and Client Records, Revenues and Benefits Solution/Interface
- Interface to Education Management System
- Interface to NHS/Health Systems
- Interface to Emergency Services (Police, Ambulance Fire) Systems
- Interface to Social Landlords/Housing Systems
- Interface to Public Health Systems
- Interface to Transport Systems
- Interface to Schools Systems

b) Describe the composition of their overall solution indicating how each element/module/function is delivered i.e. is it:

- Fully integrated into the core product
- A 'bolt-on' module

- An interface solution
- Third-party software
- Other/hybrid solution

Tenderers are invited to outline their responses in the pricing section of the Specification of Requirements and Tender Response document – Appendix 1.
Tenderers will be evaluated on the Whole Life Cost only and further detail about scoring and evaluation can be found in Section 5. Tenderers will, however, provide costed details on each of the integrations, modules and any interfaces to third parties that are included in the Whole Life Cost. The Council needs to be more informed about those component costs when undertaking some key business decisions in respect of its Digital Transformation Programme; some of the systems and interfaces currently in use may not be required/used in the future. The Council, therefore, reserves the right not to purchase or pay the relevant cost in relation to all elements/modules/interfaces that may be included within the Whole Life Cost.

2.0) Submission of Tender Process and Documents

2.1 Instructions for Tendering

You are invited to tender for the provision of an integrated Adults and Children's Social Care System under the CCS Framework RM 1059 – Lot 6

2.1.1

Tenders are to be submitted in accordance with the RM1059 framework terms and conditions and the instructions outlined within this document.

2.1.2

Tenders must be submitted in accordance with the following instructions. Tenders not complying in any particular way may be rejected by Shropshire Council (the Council) whose decision in the matter shall be final. Persons proposing to submit a Tender are advised to read the Invitation to Tender documentation carefully to ensure that they are fully familiar with the nature and extent of the obligations to be accepted by them if their Tender is accepted.

2.1.3

The Invitation to Tender documents must be treated as private and confidential. Tenderers should not disclose the fact that they have been invited to tender or release details of the Invitation to tender document other than on an "in confidence" basis to those who have a legitimate need to know or who they need to consult for the purpose of preparing the tender as further detailed in these Instructions for Tendering.

2.1.4

Tenderers shall not at any time release information concerning the invitation to tender and/or the tender documents for publication in the press or on radio, television, screen or any other medium without the prior consent of the Council.

2.1.5

The fact that a Tenderer has been invited to submit a tender does not necessarily mean that it has satisfied the Council regarding any matters raised in the pre-tender questionnaire submitted under the CCS framework RM1059. The Council makes no representations regarding the Tenderer's financial stability, technical competence or ability in any way to carry out the required services. The right to return to any matter raised in the pre-tender questionnaire submitted as part of the formal tender evaluation relating against to the CCS framework RM1059 is hereby reserved by the Council.

2.1.6

The Invitation to Tender is issued on the basis that nothing contained in it shall constitute an inducement or incentive nor shall have in any other way persuaded a tenderer to submit a tender or enter into a Contract or any other contractual agreement.

2.1.7

Shropshire Council is purchasing on behalf of itself and any wholly owned local authority company or other entity that is deemed to be a contracting authority by virtue of the Council's involvement

Terms and Conditions

2.1.8

Every Tender received by the Council shall be deemed to have been made subject to the framework Terms and Conditions and these Instructions for Tendering unless the Council shall previously have expressly agreed in writing to the contrary.

2.1.9

The Tenderer is advised that in the event of their Tender being accepted by the Council, they will be required to supply the required goods and services.

Preparation of Tenders

2.1.10

Tenders should be submitted using the Specification of Requirements and tender response (Appendix 1) following the instructions given towards the front of the document. The Tenderer's attention is specifically drawn to the date and time for receipt of Tenders and that no submission received after the closing time will be considered.

2.1.11

All documents requiring a signature must be signed;

a) Where the Tenderer is an individual, by that individual;
b) Where the Tenderer is a partnership, by two duly authorised partners;
c) Where the Tenderer is a company, by two directors or by a director and the secretary of the company, such persons being duly authorised for the purpose.

2.1.12

The Invitation to Tender Documents are and shall remain the property and copyright of the Council

Tender preparation and costs

2.1.13

It shall be the responsibility of Tenderers to obtain for themselves at their own expense all information necessary for the preparation of their Tender. No claim arising out of want of knowledge will be accepted. Any information supplied by the Council (whether in the Tender Documentation or otherwise) is supplied only for general guidance in the preparation of tenders.

2.1.14

Any Tenderer considering making the decision to enter into a contractual relationship with the Council must make an independent assessment of the Tender opportunity after making such investigation and taking such professional advice as it deems necessary.

2.1.15

Tenderers will be deemed for all purposes connected with their Tender submission where appropriate to have visited and inspected the Council, its assets, all the locations in respect of the delivery of the services/supplies/works and to have satisfied themselves sufficiently as to the nature, extent and character of the services supplies/works sought, and the human resources, materials, software, equipment, machinery, and other liabilities and other matters which will be required to perform the contract.

2.1.16

The Council will not be liable for any costs incurred by Tenderers in the preparation or presentation of their tenders.

2.1.17

Tenderers are required to complete all pricing detail in the Invitation to tender documents (Appendix 1). The terms “Nil” and “included” are not to be used but a zero or figures must be inserted against each item. Unit rates and prices must be quoted in pounds sterling and whole new pence.

2.1.18

It shall be the Tenderer’s responsibility to ensure that all calculations and prices in the Tender documentation are correct at the time of submission.

2.1.19

The Tenderer is deemed to have made him/herself acquainted with the Council’s requirements and tender accordingly. Should the Tenderer be in any doubt regarding the true meaning and intent of any element of the specification he is invited to have these fully resolved before submitting his Tender. No extras will be allowed for any loss or expense involved through any misunderstanding arising from his/her failure to comply with this requirement.

2.1.20

Any Tender error or discrepancy identified by the Council shall be drawn to the attention of the Tenderer who will be given the opportunity to correct, confirm or withdraw the Tender.

2.1.21

The Tender Documents must be treated as private and confidential. Tenderers should not disclose the fact that they have been invited to tender or release details of the Tender document other than on an in Confidence basis to those who have a legitimate need to know or whom they need to consult for the purpose of preparing the Tender.

Parent Company Guarantee

2.1.22

It is a condition of contract that if the tendering company is a subsidiary then its Ultimate Group/Holding Company must guarantee the performance of this contract and provide a letter to that effect signed by a duly authorised signatory of the Ultimate Group/Holding Company if requested to do so by the Council. Where the direct parent company cannot provide an adequate guarantee in the opinion of the Council, the Council will look to another group or associate company, with adequate assets, to be the guarantor. In cases where the contract is with a Joint Venture Company (JVC) or a Special Purpose Vehicle (SPV) company, which may have two or more parent companies and which may not be adequately capitalised or have sufficient financial strength on its own to support the risk and obligations it has under the contract, ‘joint and several’ guarantees / indemnities from the parent companies of the JVC or SPV may be sought.

Warranty

2.1.23

The Tenderer warrants that all the information given in their Tender and their request to Participate Questionnaire submitted in relation to framework RM1059 is true and accurate. The information provided will be deemed to form part of any contract formed under this contract.

The Tenderer warrants that none of their current Directors have been involved in liquidation or receivership or have any criminal convictions

Tender submission

2.1.24

Tenders must be submitted strictly in accordance with the letter of instruction accompanying this Invitation to Tender. Tenders must be submitted by the deadline of **noon, 11th November 2016.**

2.1.25

No unauthorised alteration or addition should be made to the Requirements Specification and Tender Response Document, or to any other component of the Tender document. If any such alteration is made, or if these instructions are not fully complied with, the Tender may be rejected.

2.1.26

Qualified tenders may be submitted, but the Council reserves the right not to accept any such tender. The Council's decision on whether or not a Tender is acceptable will be final.

2.1.27
Tenderers should note that their Tender must remain open and valid and capable of acceptance for a period of at least 90 days

2.1.28
Tenderers should note that Tenders and supporting documents must be written in English and that any subsequent contract, which may or may not be entered into, its formation, interpretation and performance, shall be subject to and in accordance with the laws of England and subject to the jurisdiction of the Courts of England and Wales.

2.1.29
Where Tender submissions are incomplete the Council reserves the right not to accept them.

Tender Evaluation

2.1.30
Tenderers may be called for interview to seek clarification of their tender or additional or supplemental information in relation to their tender. Presentations, site visits and demonstrations will be used to clarify and moderate issues raised in the Tenderer's submissions. Any areas of discrepancy between submissions and information gained from the presentations, site visits and demonstrations will be reviewed and scores previously awarded will be amended if necessary.

2.1.31
If the Council suspects that there has been an error in the pricing of a Tender, the Council reserves the right to seek such clarification, as it considers necessary from the Tenderer in question.

Clarifications

2.1.32
Tenderers are responsible for clarifying any aspects of the tendering process and/or the Invitation to Tender documents in the manner described below.

2.1.33
If you are unsure of any section and require further clarification, please contact us via our Delta Tender box.

2.1.34
Where appropriate, an Authorised Officer may direct the Tenderer to other officers to deal with the matter.

2.1.35
All queries should be raised as soon as possible (in writing), in any event not later than **2nd November 2016.**

2.1.36
All information or responses that clarify or enhance the tendering process will be supplied to all Tenderers on a uniform basis (unless expressly stated otherwise). These responses shall have the full force of this Instruction and where appropriate the Conditions of Contract. If a Tenderer wishes the Council to treat a question as confidential this must be expressly stated. The Council will consider such requests and will seek to act fairly between the Tenderers, whilst meeting its public law and procurement duties in making its decision.

2.1.37
Except as directed in writing by the Authorised Officer, and confirmed in writing to a Tenderer, no agent or officer or elected Member (Councillor) of the Council has any express or implied authority to make any representation or give any explanation to Tenderers as to the meaning of any of the

Tender Documents, or as to anything to be done or not to be done by a Tenderer or to give any warranties additional to those (if any) contained in the ITT or as to any other matter or thing so as to bind the Council in any way howsoever.

Continuation of the Procurement Process

2.1.38

The Council shall not be committed to any course of action as a result of:

a) Issuing this Invitation to Tender;

b) Communicating with a Tenderer, a Tenderer's representative or agent in respect of this procurement exercise;

c) Any other communication between the Council (whether directly or through its agents or representatives) and any other party.

2.1.39
The Council reserves the right at its absolute discretion to amend, add to or withdraw all, or any part of this Invitation to Tender at any time during the tendering stage of this procurement exercise.

2.1.40
At any time before the deadline for receipt of tender returns the Council may modify the Invitation to Tender by amendment. Any such amendment shall be numbered and dated and issued by the Council to all participating tenderers. In order to give prospective Tenderers reasonable time in which to take the amendment into account in preparing its Tender return, the Council may in its sole discretion, extend the deadline for submission of the tender returns.

2.1.41
The Council reserves the right to amend, withdraw, terminate or suspend all or any part of this procurement process at any time at its sole discretion.

Confidentiality

2.1.42
All information supplied by the Council in connection with or in these Tender Documents shall be regarded as confidential to the Council unless the information is already within the public domain or subject to the provisions of the Freedom of Information Act 2000.

2.1.43
The Contract documents and publications are and shall remain the property of the Council and must be returned upon demand.

2.1.44
Tenderers shall ensure that each and every sub-contractor, consortium member and/or professional advisor to whom it discloses these papers comply with the terms and conditions of this ITT.

2.1.45
The contents of this Invitation to Tender are being made available by the Council on condition that:

a) Tenderers shall at all times treat the contents of the Invitation to tender and any related documents as confidential, save in so far as they are already in the public domain and Tenderers shall not, subject to the provisions relating to professional advisors, sub-contractors or other persons detailed below, disclose, copy, reproduce, distribute or pass any of the contents of the Invitation to tender to any other person at any time or allow any of these things to happen;

b) Tenderers shall not use any of the information contained in this Invitation to tender for any purpose other than for the purposes of submitting (or deciding whether to submit) the tender

c) Tenderers shall not undertake any publicity activity within any section of the media.

2.1.46

Tenderers may disclose, distribute or pass this Invitation to tender to their professional advisors, sub-contractors or to another person provided that:

a) This is done for the sole purpose of enabling an Invitation to tender to be submitted and the person receiving the Information undertakes in writing to keep the Invitation to Tender confidential on the same terms as if that person was the Tenderer; or

b) The Tenderer obtains the prior written consent of the Council in relation to such disclosure, distribution or passing of the Invitation to Tender; or

c) The disclosure is made for the sole purpose of obtaining legal advice from external lawyers in relation to the procurement or to any Contract(s) which may arise from it; or

d) The Tenderer is legally required to make such a disclosure.

2.1.47

The Council may disclose detailed information relating to the Invitation to Tender to its officers, employees, agents, professional advisors or Governmental organisations and the Council may make any of the Contracts and procurement documents available for private inspection by its officers, employees, agents, professional advisors, contracting authorities or Governmental organisations.

Transparency of Expenditure

2.1.48

Further to its obligations regarding transparency of expenditure, the Council may be required to publish information regarding tenders, contracts and expenditure to the general public, which could include the text of any such documentation, except for any information which is exempt from disclosure in accordance with the provisions of the Freedom of Information Act to be determined at the absolute discretion of the Council.

Freedom of Information

2.1.49

Please note that from 1 January 2005 under the provisions of the Freedom of Information Act 2000, the public (included in this are private companies, journalists, etc.) have a general right of access to information held by public authorities. One of the consequences of those new statutory responsibilities is that information about your organisation, which Shropshire Council may receive from you during this tendering process may be subject to disclosure, in response to a request, unless one of the various statutory exemptions applies.

2.1.50

In certain circumstances, and in accordance with the Code of Practice issued under section 45 of the Act, Shropshire Council may consider it appropriate to ask you for your views as to the release of any information before we make a decision as to how to respond to a request. In dealing with requests for information under the Act, Shropshire Council has to comply with a strict timetable and it would therefore expect a timely response to any such consultation within five working days.

2.1.51

If, at any stage of this tendering process, you provide any information to Shropshire Council in the expectation that it will be held in confidence, then you must make it clear in your documentation as to the information to which you consider a duty of confidentiality applies. The use of blanket protective markings such as “commercial in confidence” will no longer be appropriate and a clear indication as to what material is to be considered confidential and why it should be given.

2.1.52

Shropshire Council will not be able to accept that trivial information or information which by its very nature cannot be regarded as confidential should be subject to any obligation of confidence.

2.1.53

In certain circumstances where information has not been provided in confidence, Shropshire Council may still wish to consult with you as to the application of any other exemption such as that relating to disclosure that will prejudice the commercial interests of any party. However, the decision as to what information will be disclosed will be reserved to Shropshire Council.
For guidance on this issue see: http://www.ico.gov.uk

Disqualification

2.1.54

The Council reserves the right to reject or disqualify a Tenderer's Tender submission where:

a) The tenderer fails to comply fully with the requirements of this Invitation to tender or is in breach of any legislation relating to Bribery and Corruption or is guilty of a serious or intentional or reckless misrepresentation in supplying any information required; or

b) The tenderer is guilty of serious or intentional or reckless misrepresentation in relation to its tender return and/or the procurement process.

c) The tenderer directly or indirectly canvasses any member, official or agent of the Council concerning the award of the contract or who directly or indirectly obtains or attempts to obtain information from any such person concerning any other Tender or proposed Tender for the services. The Canvassing Certificate must be completed and returned as instructed.

d) The Tenderer:

1. Fixes or adjusts the amount of his Tender by or in accordance with any agreement or arrangements with any other person; or

2. Communicates to any person other than the Council the amount or approximate amount of his proposed Tender (except where such disclosure is made in confidence in order to obtain quotations necessary for preparation of the Tender for insurance purposes); or

3. Enters into an agreement or arrangement with any other person that he shall refrain from tendering or as to the amount of any Tender to be submitted; or

4. Offers or agrees to pay or give or does pay or gives any sum of money, inducement or valuable consideration directly or indirectly to any person for doing or having done or causing or having caused to be done in relation to any Tender or proposed Tender for the services any act or omission.

2.1.55

Any disqualification will be without prejudice to any other civil remedies available to the Council and without prejudice to any criminal liability which such conduct by a Tenderer may attract. The Non-Collusive Tendering Certificate must be completed and returned as instructed.

2.1.56

The Council reserves the right to disqualify an Applicant from further participating in this procurement process where there is a change in the control or financial stability of the Tenderer at any point in the process up to award of a contract and such change of control or financial stability has a materially adverse effect on the Tenderer's financial viability or ability to otherwise meet the requirements of the procurement process.

E-Procurement

2.1.57

As part of its procurement strategy Shropshire Council is committed to the use of technology that can improve the efficiency of procurement. Successful Tenderers may be required to send or receive documents electronically. This may include purchase orders, acknowledgements, invoices, payment advices, or other procurement documentation. These will normally be in the Council's standard formats, but may be varied under some circumstances so as not to disadvantage small and medium suppliers.

Award of Contract

2.1.58 Award Criteria

The Award Criteria has been set out within this invitation to tender. The Council is not bound to accept the lowest or any Tender.

2.1.59 Award Notice

The Contracting Authority reserves the right to pass all information regarding the outcome of the Tendering process to the Office of Fair Trading to assist in the discharge of its duties. Additionally, the Council will adhere to the requirements of the Freedom of Information Act 2000 and Tenderers should note this statutory obligation.

2.1.60 Transparency of Expenditure

Further to its obligations regarding transparency of expenditure, the Council may also be required to publish information regarding tenders, contracts and expenditure to the general public, which could include the text of any such documentation, except for any information which is exempt from disclosure in accordance with the provisions of the Freedom of Information Act to be determined at the absolute discretion of the Council.

2.1.61 Value of Contract

Shropshire Council cannot give any guarantee in relation to the value of this contract.

2.1.62 Acceptance

Tenders must be submitted strictly in accordance with the terms of the Council's Invitation to Tender documentation and acceptance of the tender shall be conditional on compliance with this Tender Condition.

2.1.63 Tender Documentation

The Tender documentation including, the framework Terms and Conditions of Contract, the Tender Response document, these Instructions to Tender, together with the formal written acceptance by the Council will form a binding agreement between the Contractor and the Council.

2.1.64 Provision and Supply of Services

The Tenderer shall be prepared to commence the provision of the supply and services on the start date of the contract arrangement being 1st February 2017.

Payment Terms

2.1.65

Tenderers should particularly note that the principles governing public procurement require that, as far as is reasonably possible, payments for Goods, Works or Services are made after the provision. Therefore, any indication of a pricing strategy within a Tender which provides for substantial payments at the outset of the Contract will be examined carefully to decide whether or not a Tender in such form can be accepted. If in the opinion of the Council such substantial payments appear excessive in relation to the requirements of the Contract the Council reserves, without prejudice to any other right to reject any Tender it may have, the right to require the Tenderer to spread such proportion of the costs as are considered excessive over the duration of the Contract.

Liability of Council

2.1.66

The Council does not bind himself to accept the lowest or any tender.

2.1.67

The Council does not accept any responsibility for any pre-tender representations made by or on its behalf or for any other assumptions that Tenderers may have drawn or will draw from any pre-tender discussions.

2.1.68

The Council shall not be liable to pay for any preparatory work or other work undertaken by the Tenderer for the purposes of, in connection with or incidental to this Invitation to Tender, or submission of its Tender response or any other communication between the Council and any other party as a consequence of the issue of this Invitation to Tender.

2.1.69

The Council shall not be liable for any costs or expenses incurred by any Tenderer in connection with the preparation of a Tender return for this procurement exercise, its participation in this procurement whether this procurement is completed, abandoned or suspended.

2.1.70

Whilst the Tender Documents have been prepared in good faith, they do not purport to be comprehensive nor to have been formally verified. Neither the Council nor any of its staff, agents, elected Members, or advisers accepts any liability or responsibility for the adequacy, accuracy or completeness of any information given, nor do they make any representation or give any warranty, express or implied, with respect to the Tender Documents or any matter on which either of these is based (including, without limitation, any financial details contained within the Specification and Contract Documentation). Any liability is hereby expressly disclaimed save in the event of fraud, or in the event of specific warranties provided within the Contract Documentation.

The Contractor agrees that where requested in writing during the term of any Agreement for the supply of Goods, Works or Services it will ensure that an appropriately authorised representative of the Contractor shall attend a Committee meeting of the Council upon being invited to do so by the Council

Declaration

2.1.71

We, as acknowledged by the signature of our authorised representative, accept these Instructions to Tender as creating a contract between ourselves and the Council. We hereby acknowledge that any departure from the Instructions to Tender may cause financial loss to the Council

Signed (1) ………………………………… Status…………………………………………

Signed (2) ………………………………… Status…………………………………………

(For and on behalf of ……………………………………………………………)

Date ……………………………………

2.2 Non-Canvassing Certificate

Non – Canvassing Certificate

Non-Canvassing Certificate

To: Shropshire Council (hereinafter called "the Council")

I/We hereby certify that I/We have not canvassed or solicited any member officer or employee of the Council in connection with the award of this Tender of any other Tender or proposed Tender for the Services and that no person employed by me/us or acting on my/our behalf has done any such act.

I/We further hereby undertake that I/We will not in the future canvass or solicit any member officer or employee of the Council in connection with the award of this Tender or any other Tender or proposed Tender for the Services and that no person employed by me/us or acting on my/our behalf will do any such act.

Signed (1) ……………………………… Status………………………………………

Signed (2) ……………………………… Status………………………………………

(For and on behalf of ………………………………………………………….)

Date …………………………………….

2.3 Non - Collusive Tendering Certificate

Non – Collusive Tendering Certificate

Non-collusive Tendering Certificate

To: Shropshire Council (hereinafter called "the Council")

The essence of selective tendering is that the Council shall receive bona fide competitive Tenders from all persons tendering. In recognition of this principle:

I/We certify that this is a bona fide Tender, intended to be competitive and that I/We have not fixed or adjusted the amount of the Tender or the rates and prices quoted by or under or in accordance with any agreement or arrangement with any other person.

I/We also certify that I/We have not done and undertake that I/We will not do at any time any of the following acts: -

(a) communicating to a person other than the Council the amount or approximate amount of my/our proposed Tender (other than in confidence in order to obtain quotations necessary for the preparation of the Tender for insurance); or

(b) entering into any agreement or arrangement with any other person that he shall refrain from Tendering or as to the amount of any Tender to be submitted; or

(c) offering or agreeing to pay or give or paying any sum of money, inducement or valuable consideration directly or indirectly to any person for doing or having done or causing or having caused to be done in relation to any other Tender or proposed Tender for the Services any act or omission.

Signed (1) .... Status...

Signed (2) .... Status...

(For and on behalf of ....)

Date ....

2.4 Declaration of Connection with Officers or Elected Members of the Council

Declaration of Connection with Officers or Elected Members of the Council

Are you or any of your staff who will be affected by this invitation to tender related or connected in any way with any Shropshire Council Elected Councillor or Employee?

Yes / No *If yes, please give details:*

Name	Relationship

Please note:

This information is collected to enable the Council to ensure that tenders are assessed without favouritism. Whether or not you have a connection with elected members or employees will have no bearing on the success of your tender, but your tender will not be considered unless this declaration has been completed.

Signed (1) ……………………………… Status………………………………………

Signed (2) ……………………………… Status………………………………………

(For and on behalf of ……………………………………………………………..)

Date ……………………………………..

2.5 Supplier Information

Supplier Information

1.1 Supplier details	**Answer**	
Full name of the Supplier completing the Tender		
Registered company address		
Registered company number		
Registered charity number		
Registered VAT number		
Name of immediate parent company		
Name of ultimate parent company		
Please mark ‘X’ in the relevant box to indicate your trading status	i) a public limited company	□ Yes
	ii) a limited company	□ Yes
	iii) a limited liability partnership	□ Yes
	iv) other partnership	□ Yes
	v) sole trader	□ Yes
	vi) other (please specify)	□ Yes

Please mark 'X' in the relevant boxes to indicate whether any of the following classifications apply to you	i)Voluntary, Community and Social Enterprise (VCSE)	▢ Yes
	ii) Small or Medium Enterprise (SME) [1]	▢ Yes
	iii) Sheltered workshop	▢ Yes
	iv) Public service mutual	▢ Yes

1.2 Contact details	
Supplier contact details for enquiries about this tender	
Name	
Postal address	
Country	
Phone	
Mobile	
E-mail	

2.6 Tender Response Checklist

Reference	**Item**	**Completed by Tenderer (Signature)**
2.2	NON-CANVASSING CERTIFICATE	
2.3	NON-COLLUSIVE TENDERING CERTIFICATE	
2.4	DECLARATION OF CONNECTION WITH OFFICERS OR ELECTED MEMBERS OF THE COUNCIL	
2.5	SUPPLIER INFORMATION	
2.7	FORM OF TENDER SIGNED	
Appendix 1	SPECIFICATION OF REQUIREMENTS, PRICING SCHEDULE AND TENDER RESPONSE	

2.7 Form of Tender

Form of Tender

Form of Tender

Shropshire Council

We confirm that this, our tender, represents an offer to Shropshire Council that if accepted in whole, or in part, will create a binding contract for the supply of a Social Care System at the prices and terms agreed and subject to the terms of the invitation to tender documentation and the framework terms RM1059 Lot 6, copies of which we have received.

Signed ………………………………. Name…………………………………………...

Date ………………………………….

Designation ……………………………………………….

Company…………………………………………………….

Address ……………………………………………………………………………………….

………………………………………………………………………………………………….

……………………………………….. Post Code ………………………………………

3.0) Procurement Time Table

ACTION	COMPLETION DATE
Preparation	
ITT issued to market	October 4 2016
Framework Suppliers to inform that they intend to bid	October 14 2016
Final date for submission of clarification questions from Suppliers	Deadline November 2 2016
Final date for responses to clarification questions to be provided to Suppliers	Latest November 7 2016
ITT submissions from Suppliers – 12 noon	November 11 2016
Initial evaluation	November 25 2016
Clarification questions to Suppliers	November 25 2016
Responses from Suppliers	December 2 2016
Short List Suppliers and notify those not short listed, to be completed by	December 9 2016
Supplier Presentations (to be completed between the date of shortlisting and 23rd December)	December 9 - 23 2016
Supplier Reference site visits (to be completed between the date of shortlisting and 23rd December)	December 9 - 23 2016
Final questions to Supplier and evaluation of Supplier responses, to be completed by	January 6 2017
Select Preferred Supplier	January 11 2017
Agree Final Contract detail & Notification of award decision	January 18 2017
Standstill Period	January 30 2017
Contract Signature	February 1 2017

4.0) Contract Period

The successful bidder will be responsible for providing this service for a period of five years with an option to extend for up to a further two years at the Councils sole discretion, commencing on April 1 2017

5.0) Evaluation of Tenders

5.1 Checking of Tenders

An initial examination will be made to establish the completeness of submitted tenders. The Council reserves the right to disqualify any tender submission which is incomplete.

Tenderers should satisfy themselves of the accuracy of all fees, rates and prices quoted, since Tenderers will be required to hold to these or withdraw their Tender in the event of errors being identified after the submission of Tenders.

If a Tenderer fails to provide fully for the requirements of the Specification in the Tender, it must either:

a) Absorb the costs of meeting the full requirements of the Specification within its tendered price; or
b) Withdraw its Tender

Evaluation of Tenders

As all tenderers under CCS Framework RM 1059 have already been assessed on Selection Criteria this will not be included within the evaluation for this further competition.

5.2 ITT Response Scoring and Evaluation

Introduction

Tenders will be evaluated on the answers provided to the questions outlined in the Invitation to Tender.

Scoring and evaluation will be based upon the responses contained in the Specification of Requirements and Tender Response document – Appendix 1.

Pre-requisites

Your attention is initially drawn to the pre-requisites which are outlined in the second tab of the Tender Response Document. You must be able to answer ‘YES’ to these questions in order for your response to be considered by the Evaluation Panel. If you cannot meet these pre-requisites, your tender will be excluded from the procurement process.

Additionally, most of the questions and statements included in Section 12.0 – Commercials, require you to confirm your acceptance of certain terms and conditions. Where you are unable to indicate acceptance of these terms you must provide a relevant and reasonable explanation for consideration by the Evaluation Panel. Further clarification may be sought regarding your comments to satisfy the Evaluation Panel of your ability to meet the terms and conditions.

Pricing

The Council will be looking to achieve a solution that offers the most comprehensive functionality across Adults, Children and Finance requirements and provides value for money. Please note that in scoring the tender bids across the three Groups below: functional requirements, non-functional requirements and pricing, the Council is not obliged to accept the highest scoring tender received if it is cost prohibitive and unaffordable.

5.3 Section Reference Explanation

Totals used for the scoring and evaluation methods are classified in two Phases based upon the following Group and Section apportionment of points:-

	Group	Points	Section
Phase 1	Functional Requirements	500	1.0 System Operation
			2.0 Case Management
			3.0 Adults' Specific Requirements
			4.0 Children's Specific Requirements
			5.0 Finance Requirements
			6.0 Reporting Requirements
	Non-functional Requirements	350	7.0 Technical Requirements
			8.0 Security and Audit
			9.0 Support Arrangements
			10.0 Future Developments
			11.0 Implementation, Training, Migration
			12.0 Commercials
	Pricing	200	
Phase 2	Presentations, Interactive Demonstrations & Site Visits	210	

5.4 Scoring – Phase 1

The requirements outlined in each section of the specification fall into the following categories:

a) Specific requirement
b) Open ended question
c) Value-added question

It is proposed that each of these categories is scored as follows:

5.4.1 Specific Requirements

Each specific requirement will be indicated as being either High or Medium Priority.

Tenderers are to specify which category of response, **and only one category**, they attribute to each statement of requirements on the basis of:-

A – Fully meets the requirement. Function **can** be configured by end-user or administrator.

B – Fully meets the requirement. Function **cannot** be configured by end-user or administrator

C – Fully meets the requirement only by interfacing with a 3rd party software product.

D – Partly meets the requirement. Function **can** be configured by end-user or administrator.

E – Partly meets the requirement. Function **cannot** be configured by end-user or administrator.

F – Does not meet the specified requirement

Where your response indicates that your solution **fully meets** the requirement then the functionality must exist within your current product release (non-beta) in use in at least one other local authority/client.

Each response will then be evaluated using Scoring Matrix One as follows:

5.4.2 Table 1: Scoring Matrix One

Weightings	**A**	**B**	**C**	**D**	**E**	**F**
High Priority	20	18	12	8	4	0
Medium Priority	10	9	6	4	2	0

5.4.3 Open Ended Questions

Each open ended question will be indicated as being either High or Medium Priority and is identified as open ended where appropriate in the Specification of Requirements.

Open ended questions will be evaluated using Scoring Matrix Two outlined below.

5.4.4 Value Added Questions

At the end of each section there is a ‘value-added’ question where respondents are able to outline ‘unique’ or ‘high quality’ functionality. It may be that we have omitted something from that Section and the Tenderer has provided a practical proposal. Additionally, where a solution to a requirement is not currently available, but is in development, then value added points can still be earned and under these circumstances the Tenderer is expected to provide details of the status (e.g. test, beta) of that development and an anticipated date for delivery.

Value Added Questions will be evaluated using Scoring Matrix Two outlined below.

5.4.5 Table 2: Scoring Matrix Two

Assessment	Open Ended H Priority	Open Ended M Priority	Value Added	Interpretation
Excellent	***20***	***10***	***5***	*Exceeds the requirement.* *Exceptional demonstration by the Tenderer of how they will meet this requirement by their allocation of skills and understanding, resources and quality measures. Response identifies factors that demonstrate relevant, desired and tangible added value, with evidence to support the response.*
Good	***18***	***9***	***4***	*Satisfies the requirement with minor additional benefits* *Above average demonstration by the Tenderer of how they will meet this requirement by their allocation of skills and understanding, resources and quality measures. Response identifies factors that demonstrate relevant, desired and tangible added value, with evidence to support the response.*
Acceptable	***8***	***4***	***3***	*Satisfies the requirement.* *Demonstration by the Tenderer of how they will meet this requirement by their allocation of skills and understanding, resources and quality measures, with evidence to support the response.*
Minor Reservations	***4***	***2***	***2***	*Satisfies the requirement with minor reservations* *Some minor reservations regarding how the Tenderer will meet this requirement by their allocation of skills and understanding, resources and quality measures, with limited evidence to support the response.*
Serious Reservations	***1***	***1***	***1***	*Satisfies the requirement with major reservations.* *Considerable reservations regarding how the Tenderer will meet this requirement by their allocation of skills and understanding, resources and quality measures, with little or no evidence to support the response.*
Unacceptable	***0***	***0***	***0***	*Does not meet the specification of requirements.* *Does not comply and/or insufficient information provided to demonstrate how the Tenderer will meet this requirement by their allocation of skills and understanding, resources and quality measures, with little or no evidence to support the response.*

5.5 Evaluation

Threshold One

Each respondent will need to achieve at least 20% of the overall marks available in each Section of the Specification to progress onto the next stage of evaluation. Sections 1 – 12 each contains a set of detailed requirements that collectively relate to each specific section as described in the 5.3 Section Reference table. Section 12, however, does not feature in this threshold check.

Only the marks available/achieved for the specific requirements plus the marks available/achieved for the open ended questions will be included at this stage. Value added questions are not included as these should be seen as 'bonus' points available and not specifically a points based requirement.

Threshold Two

For those who progress to the next stage the following calculations will apply to the Group points as follows:

Functional Requirements (Sections 1.0 to 6.0)

$$Group\ Score\ =\ Average\ Percentage\ Score\ (across\ all\ 6\ sections\ )\ x\ 500\ Points$$

Tenderers must pass a threshold of 250 Points

Non-Functional Requirements (Sections 7.0 to 12.0)

$$Group\ Score\ =\ Average\ Percentage\ Score\ (across\ all\ 6\ sections\ )\ x\ 350\ Points$$

Tenderers must pass a threshold of 125 Points

Pricing

$$Maximum\ Individual\ Score = 200\ Points\ for\ the\ lowest\ Whole\ Life\ Cost$$

More details on the pricing strategy are to be found below in section 5.9 Pricing Evaluation together with earlier sections 1.5 - Peripheral Systems and 1.6 Pricing - Specification of Requirements.

There is no threshold for this points section.

5.6 Calculation of Assigned Points

For the Functional and Non-functional Groups above, the final total points will be assigned to the Tenderer receiving the highest initial points in that group. All other Tenderers will be awarded final points in that Group based upon the percentage difference of their initial Group point score compared with the highest scoring Tenderer for that Group.

For example, if Tenderer 1 is the highest points scorer in the Functional Requirements Group with 400 points then they are awarded 500 points for that Group. If the next nearest Tenderer scored 300 points in the same Group, then the points awarded would reflect the fact that they have 25% fewer initial points than Tenderer 1 and would be allocated only 75% of the maximum i.e. 375 points.

For the assignment of Pricing Points, the Tenderer with the lowest Whole Life Costs – as indicated in cell E95 of the pricing schedule in Appendix 1 (see section 5.9 Pricing Evaluation for further information) will be assigned the maximum 200 points. Other Tenderers' Whole Life Costs will be assigned a percentage of the maximum points based upon the difference between the lowest Whole Life Cost Tender and their own Whole Life Costs.

Value Added Points

Any value added points earned will now be added to the Assigned Points to give a total points score for each Tenderer that has passed through thresholds 1 and 2.

This now concludes Phase 1 of the scoring and evaluation process.

5.7 Shortlisting – Phase 2

The Tenderers with the top three scores will automatically qualify to be invited to the next 'shortlisting' phase. Where a fourth Tenderer's total points score is more than 90% of the third placed Tenderer's total points score then they too will be invited to the next 'shortlisting' stage.

Tenderers who are notified that they have been short listed, will be issued with a standard brief for presentations, site visits and an interactive demonstration. A prerequisite of a reference site visit will be a visit to a local authority that has been a user of their product for 3 to 5 years and another that have had an implementation in the last 12 to 18 months. We reserve the right to visit an additional reference site of our choice.

Phase 2 of the tender evaluation process will use the Evaluation Panel to appraise Tenderers against these criteria and all members of the Evaluation Panel will represent their respective business areas. The Evaluation Panel members will use a standard scoring mechanism for presentations, demonstrations and site visits to award points as set out in Scoring Matrix Three below: -

5.7.1 Table 3: Scoring Matrix Three

Core Topic	**Feature/ Function Description**	**Points to Award for how well the feature/ function is evidenced**			
		30 Fully	**10** Not fully	**3** Partly	**0** Not at all
Ease of use	How easy it is to access the correct record(s), perform the required task(s) and accesses related records				
Operational Functions	How well the system supports the case management, financial, supervisory and reporting tasks.				
Security	Levels of system and data access security				
Workflow	How well the system manages workflow to appropriate operatives and handles prompts and reminders.				
Search facilities	How well the system supports various search tasks required to locate an appropriate record or set of records				
Help facilities	How well the system offers help, particularly when completing complex screen input				
Compliance	How well the system supports all forms of Social Care and Financial compliance				
	Totals				

5.8 Response Validation

The Tenderers may be called for interview to seek clarification of their tender or additional or supplemental information in relation to their tender. Presentations, site visits and demonstrations will be used to clarify and moderate issues raised in the Tenderer's submissions. Any areas of discrepancy between submissions and information gained from the presentations, site visits and demonstrations will be reviewed and scores previously awarded will be amended if necessary.

5.9 Pricing Evaluation

Whole Life Costs

Where the Council is looking to replace, integrate or interface to the functionality of the systems detailed in 1.5 Peripheral Systems, then this is included in the relevant sections of the Specification of Requirements and Tender Response document – Appendix 1. In this document, Tenderers are invited to explain how their solution will meet the needs of the Council in respect of 'peripheral systems', including how the proposed solution either includes/integrates the functionality of such systems or how the solution might interface to a third party system. Tenderers are expected to have priced those integrations, modules and interfaces to third parties within the full 5 year term cost of their overall system solution. **Final Selection**

The Evaluation Panel will use the assigned score from Phase 1 tender scoring, along with the above evaluation scores from the site visits, supplier presentations and interactive demonstrations to inform their preferred Tenderer choice.

Whoever scores the highest number of points accumulated from Phases 1 and 2 will be identified as the Preferred Tenderer.

6.0) Award of Contract

Any acceptance of a Tender by the Council shall be in writing.

6.1 Confidentiality

The Invitation to Tender, the Conditions of Contract and the Specification and all other documentation or information issued by the Council relating to the tender shall be treated by the Tenderer as private and confidential for use only in connection with the Tender and any resulting contract and shall not be disclosed in whole or in part to any third party without the prior written consent of the Council.

The documents which constitute the Contract and all copies thereof and shall remain the property of the Council and must not be copied or reproduced in whole or in part and must be returned to the Council on demand.

6.2 Tenderer's Warranties

In submitting a Tender, the Tenderer warrants and represents that:

It has complied in all respects with these Conditions of tender

All information, representations and other matters of fact communicated (whether in writing or otherwise) to the Council by the Tenderer or its employees in connection with or arising out of their tender are true, complete and accurate in all respects.

It had made its own investigations and research, and has satisfied itself in respect of all matters relating to the Tender, the Specification and the Conditions of Contract and that it has not submitted the Tender and will not have entered into the Contract in reliance upon any information, representations or assumptions (whether made orally, in writing or otherwise) which may have been made by the Council.

It has full power and authority to enter into the Contract and will if requested produce evidence of such to the Council.

It is of sound financial standing and the Tenderer and its partners, officers, and employees are not aware of any circumstances (other than such circumstances as may be disclosed in the accounts or other financial statements of the Tenderer which may adversely affect such financial standing in the future

6.3 Words and Expressions

Words defined in the Conditions of Contract shall have the same meaning in the invitation to Tender, the Conditions of Tender and the Specification.

7.0) Conditions of Contract

As this is a further competition under Framework RM1059 ‘Local Authority Software Solutions’ Lot 6 Social Care, the relevant Crown Commercial Service (CCS) standard call off terms and conditions apply.

Appendices

1. Specification of Requirements and Tender Response

(Please refer to separate excel document)

2. Payment Plan

This plan is subject to change dependent on the agreement of a detailed implementation plan between Preferred Supplier and the Council.

10%	Acceptance of design and implementation plan
20%	Design and Build Acceptance
30%	Test and Accept delivery of Adults, Children's and Operational Finance solution incorporating Reporting and ICT
20%	Cut over of system /Go Live
20%	Post Go Live – 3 months- Formal Contract review related to Performance measures.

3. Telford and Wrekin Council

This procurement process includes an option for Telford & Wrekin Council to award a contract under it on the same terms and conditions as awarded by Shropshire Council (should it proceed to an award of contract itself under this procurement). Should both Contracting Authorities wish to proceed to award a contract please note that the successful contractor will enter into two separate contracts one with each of the authorities. Please note the option available to Telford &Wrekin Council may not be taken up and whether this is the case or not this should not affect the bid made to Shropshire Council in any way or lead to any qualification of a bid.

More information on our population can be found at: **www.telford.gov.uk/factsandfigures**

Telford & Wrekin currently manage their adults social care records with OLM's Carefirst System. This uses Abacus to manage the financial aspects and the interface into the Council's finance system, Agresso (Unit 4). There are around 400 users of Carefirst accessing approximately 45,000 records.

Children's records are managed through Liquid Logic's Protocol. There are approximately 500 users accessing 73,000 records

The Council uses CarePath for managing the Drug and Alcohol Rehabilitation service data with approximately 70 users and 8000 records.

Shropshire Council

Corporate Information Security Policy

November 2012

Contents

SECTIONS

APPENDICES

1. Introduction

1.1. The Need for an Information Security Policy

Shropshire Council has a significant investment in computer systems and networks. In common with other organisations, to a large and continually increasing extent the Council is dependent upon the data which is stored and processed on its computers and the management information that is generated from the data.

The loss of data and computer processing facilities or breaches of data access security could incur significant costs, loss of revenue and damage to the Council's reputation as a result of:

- business activities being suspended or partially suspended;
- having to restore the data, computer programs and/or equipment;
- unauthorised disclosure of confidential information relating to individuals and/or other confidential business information being made available to 'interested parties';
- Fraudulent manipulation of cash or goods.

The preservation of confidentiality, integrity and availability of information held not only electronically within systems, but also on paper, microfiche or CD-ROM is therefore essential to the Council.

The security of the Council's information can be achieved by implementing a suitable set of controls (which comply with ISO 27001) in the form of:

- procedures;
- organisational structures;
- software functions.

specified in **Sections 4 to 11** of this policy document.

Some aspects of the Council's security will be governed by statutory legislation derived from:

- The Data Protection Act (1998)
- Copyright Designs and Patents Act (1988)
- Computer Misuse Act (1990)

In addition, external standards, such as the Government's Public Service Network Code of Connection, NHS Information Governance Toolkit and Payment Card Industry standards, also mandate that certain controls must be in in place.

Note: A glossary of terms has been put together to aid understanding of this Policy document within **Appendix A**.

1.2. Responsibility for Security

- All Council Members must accept responsibility for maintaining security standards within the organisation and adhere to the '**Acceptable Use of Electronic Services Standards'**.
- All managers[1] must accept responsibility for initiating, implementing and maintaining security standards within the organisation and adhere to the '**Acceptable Use of Electronic Services Standards**'.
- All non-managerial employees must accept responsibility for maintaining standards by conforming with those controls which are applicable to them and adhere to the '**Acceptable Use of Electronic Services Standards'**.
- ICT Services will be responsible for implementation of the controls marked for IT Specialists.
- Local managers must undertake yearly assessments of security risks within their own areas to ensure that the cost of implementation of controls is proportionate to both the value of the information and the business harm likely to result from any security breach whilst endeavouring to comply with ISO 27001.
- All employees that use information within the Council should undergo security awareness training which should include guidance on the correct use of available computer facilities.
- A mechanism for reporting losses incurred in relation to IT equipment, both on and off-site should be implemented in order to ascertain whether it would be cost effective for the Council to buy insurance cover for IT related equipment owned by the Council. The levels of loss incurred by each Service area will need to be recorded and analysed by an appointed Risk Manager. It will be the responsibility of each individual Service area to report all losses, in relation to IT equipment, to the Risk Manager.

Key to Symbols

Throughout this Policy document, employee responsibilities for all areas of Information Security have been denoted by the use of icons as follows:

💻	IT Specialist(s) or System Owners
☞	Senior Officers within service areas (including Line Managers & IT Managers)
☺	All Users

[1] A Manager is anyone who has responsibility for managing employees; the word manager may not appear in their job title.

2. Scope

2.1. In Scope

This Policy will become a Code of Practice for all Council service areas unless listed as Out of Scope.

The policy will specify guidelines for:

- System access control
- Communications and operations management
- Systems development and maintenance
- Personnel security
- Physical and environmental security
- Asset classification
- Business continuity planning
- Compliance with legislation

2.2. Out of Scope

The following area will not be addressed in this Policy:

- IT Security in Schools

3. Policy Objectives

The objectives of this Policy are:

- To ensure the preservation of **confidentiality**, **integrity** and **availability** of Council information and protection of assets. This can be achieved by providing Management with the necessary direction and support for the implementation and maintenance of the necessary information security controls;
- To ensure that the Council's Officers are aware of their responsibilities and the commitments required in order to comply with the requirements specified in the Policy.

4. System Access Control

4.1 User Access Management

4.1.1. User Registration and Review of User Access Rights 💻 ☞

A formal user registration and termination process should be in place for all information systems and include:

- Allocation of a unique user ID to all users. Group identifiers should only be permitted where the work required of a team cannot otherwise be carried out or where service levels would be severely affected by allocating employees with unique identifiers;
- Checking that a new user registration has been authorised by the appropriate manager and ensuring that access to appropriate information systems is denied until the authorisation process has been completed;
- Checking that the level of access requested is appropriate to the user role and does not compromise segregation of duties;
- Providing users with details of access rights granted to them;
- Ensuring that all users have signed a statement indicating that they have understood the conditions of access prior to being given access to the appropriate information systems.
- Maintaining a record of all registered users;
- The appropriate manager should review user's access rights at least every 6 months or after any major employee changes. ICT Services should be notified promptly and remove access rights for users who have changed jobs or left the organisation either temporarily or permanently and periodically check for and remove redundant user IDs;
- Ensuring that redundant user IDs are not re-issued.

4.1.2. *Third Party Access* 💻 ☞

Sharing of the Council's networks to the degree that it (sharing) extends beyond the organisation's boundaries requires both adequate management of the situation and logical controls in place in order to protect the Council from the risks of unauthorised access and sabotage. The logical controls required are specified under the **section 4.3.2 - *Network Routing Controls for Third Party Access***. To adequately manage the third party arrangements, managers within each Service area should ensure that an agreement is in place with any supplier requiring access to the Council's systems for maintenance work or to perform upgrades. The agreement should inform the supplier of the terms under which the work is to be performed and should include:

- details of permitted access methods;
- details of the authorisation process for Third Party access and types of privileges to be assigned;
- supervision of all work performed at the Council's premises.

4.1.3. *Privilege Management* 💻 ☞

Privileges are a means of controlling user access to both functionality and system manager utilities within information systems/applications. The following controls should be adhered to in the process of managing privileges:

- They should be allocated to employees on a need-to-use basis, i.e. the minimum requirement for their functional role;
- A record of all privileges allocated should be maintained and include details of user ID, functions accessible to the user and access type (create, read, update and delete);
- Authorisations for special privileged access rights (users with create, update & delete capabilities who are either contract or temporary employees or maintenance personnel from a third party supplier) should be reviewed at least every 6 months and checks made specifically to ensure that unauthorised privileges have not been obtained.

4.1.4. *User Password Management* 💻 ☞

Passwords are a means by which a user ID is validated prior to being given access to a system. Passwords should be controlled through a formal management process which:

- requires users to sign an undertaking to keep passwords confidential and where group passwords are being utilised to keep them solely within members of the group;
- ensures that each time a new user is registered they are given a secure temporary password which they are forced to change immediately upon log-in (where technically possible). Temporary passwords issued when users forget their password should only be provided following positive identification of the user.

4.1.5. *Logical Password Management* 💻

Passwords should:

- not be displayed to the screen when being entered by a user;
- be stored in encrypted form wherever possible and transmitted via our own routed networks or VPN networks via the Internet;
- be amended immediately following installation of software if set up purely for a supplier to use whilst undertaking work for the Council.

4.1.6. *User Responsibilities (Password Management)* ☺

All users should follow the guidelines below when selecting and using passwords in order to help mitigate the risk of unauthorised access to the Council’s information systems:

- passwords should be kept confidential;
- keeping paper records of passwords should be avoided unless they can be stored securely;

- passwords should be changed regularly (preferably every 60 days) depending on the sensitivity/business importance of the information contained within a system;
- the use of mixed case alphanumeric passwords should be adopted by all users because in this format they are significantly harder to crack. The minimum requirements are that users select quality passwords of at least 8 characters in length which should be;
  - easy to remember
  - free from identical or consecutive characters or numbers
  - not based on anything which could be guessed easily by someone or obtained from personal information such as name, telephone number or date of birth.
- Any automated log-on process should not include passwords e.g. stored as a function key or macro.
- Each individual should use a unique password for each different service they have access to.
- **Whenever prompted by ‘Windows’ to ‘Save Password’; never do so.**

4.1.7. *User Responsibilities for Access Control of Unattended Equipment* ☺

All users should ensure that equipment installed in the Council’s offices is adequately protected from unauthorised access when left unattended or when the office is unoccupied by other employees.

Users should adhere to the following rules when leaving workstations or servers unattended:

- All active sessions should be terminated unless they can be secured by an appropriate locking mechanism such as a password protected screensaver.
- Terminate all sessions tidily i.e. don’t just switch the PC off.

4.1.8. *User Responsibilities - Access Control of Unattended (Off-Site Equipment)*

☺

The following guidelines should be followed for all Council owned IT equipment located off-site:

- all active sessions should be terminated when laptops or workstations are left unattended unless they can be secured by an appropriate locking mechanism such as a password protected screensaver;
- all workstations located at home and not linked to the corporate network (including laptops) which are used to store data should be further protected by the use of a power-on password;
- anti-virus software must be used on all machines and updated regularly (as and when updates are available by ICT Services);

See **Section *8.2.5 - Security of Equipment Off-Premises*** for more general controls.

NOTE: Screensaver and power-on password settings should always be switched off as and when maintenance work is to be carried out by ICT Services.

4.2 Application Access Control

In order to prevent unauthorised access to information stored in information systems; logical access to systems functions should be restricted to authorised users via the following measures:

- By applying the procedures relating to user access (detailed in **Section 4.1.3 - *Privilege Management)*** to user profiling as a means of controlling create, view, update and delete access to sensitive menu options.

4.2.1. *Monitoring of Application Access* 💻

To detect any unauthorised activities and to ensure conformity to the user access management procedures detailed in **Section 4.1**, audit logs should be produced (not necessary to print) for all high risk applications, where possible. High risk applications are those which store sensitive, personal or financial based data and will be identified via the risk assessment process undertaken by each Service area on a yearly basis.

The logs should be kept for an agreed period of time (determined by the Service area in consultation with Internal Audit) in order to assist in future investigations. They should be reviewed regularly by the system managers and periodically by the Information Governance Officer on behalf of all Service areas. A log should provide the following information for each transaction:

- associated user ID;
- dates and times for logging on and off;
- where applicable an Indicator to show a failed log on attempt;
- associated screen or function Identifier being accessed;

4.2.2. Clock Synchronisation 💻

In order to ensure the accuracy of audit logs, the correct setting of application clocks is important.

Where a PC or server has the capability to operate a real-time clock, it should be set to an agreed standard such as Universal Co-ordinated Time (UCT).

Some PC clocks will drift with time. Therefore a procedure should be put in place which checks for and corrects any variations on any machine linked to the corporate network.

4.3 Network Access Control

Access to internal and external networked services should be strictly controlled in order to ensure that the security of Council services is not compromised in any way.

Networks are designed to allow maximum scope for sharing resources and flexibility of routing, but at the same time these features provide an ideal opportunity for abuse unless adequate controls are put in place. Therefore, ICT Services in consultation with the Service areas for whom they are running networked services should implement the following controls:

4.3.1. *User & Node Authentication for External Connections* 💻

Any access to the Council's systems by remote users should be subject to verification of authenticity. This can be achieved by either checking the user address (IP address/user ID) via the firewall user validation routines or checking connections to remote systems are authentic.

4.3.2. *Network Routing Controls for Third Party Access* 💻

Routing controls should be implemented for third party links with Council systems to ensure that computer connections and information flows do not breach the Access Control Policy eg currently the use of modems or remote control software is not permitted on any 'network attached' server or workstation.

The routing controls should be based on positive source and destination address checking mechanisms.

Alternatively, network address translation can be implemented to isolate the networks and prevent routes from propagating from the network of a supplier's organisation into the Council's networks.

4.3.3. Operating System Access Control 💻

The following security facilities at operating system level should be used to restrict access by unauthorised parties to the Council's computer resources:

- terminal log-on procedures should be documented for all operating systems. A log-on procedure where possible, should:
  - not display system or application identifiers until the log-on process has been successfully completed;
  - display a general notice to the terminal screen warning that the computer should only be accessed by authorised users;
  - not provide help messages during the log-on procedure that would aid an unauthorised user;
  - limit the number of unsuccessful log-on attempts allowed to five and subsequently disable that user ID;
  - record all unsuccessful attempts on an audit trail (if system resources make this practical).
- all passwords should be validated against the user ID for authentication;
- system utilities such as start-up or back-up routines and log-on scripts should only be made available to relevant users;
- all use of system utilities should be logged on an audit trail or by other means where possible.

4.3.4. Internet Access Control 💻 ☞

The following controls should be implemented to restrict the manner in which users can access the Internet:

- all users should be given a unique user ID;
- ICT Services should set a password at the outset which contains both alpha and numeric characters thus making it harder to crack;
- users accessing the Internet via the Corporate Network (as opposed to a standalone machine) should have the ‘Save Password’ utility disabled;
- the user ID and password should be validated prior to access to Internet services being granted;
- all user Internet communications (including incoming/outgoing E-mail transactions) via the Council’s firewall should be logged and analysed on a weekly basis. The following minimum set of data should be recorded:
  - user ID or e-mail address
  - destination address
  - date
  - time
  - action
  - status (accepted or rejected)
- all monitoring software settings should be fully documented and all word searching criteria reassessed at least every 6 months. Web address should be added or withdrawn as and when the Council are notified of new or defunct sites.

NOTE:

Please see **Appendix B** - ***Internet Acceptable Use Policy*** for user initiated and other Internet Controls

5. Communications & Operations Management

Responsibilities and procedures for the management and operation of all computers and networks should be established. This includes:

- production of a set of fully documented and up-to-date operational guidelines;
- capacity planning in order to reduce the risk of system overload;
- documented precautions to be taken in order to detect and prevent computer viruses on PCs;
- production of security controls governing the management of networks;
- implementation of procedures and standards to protect information and media in transit.

5.1 Operational Procedures and Responsibilities

5.1.1. *Documented Operating Procedures* 💻

Procedures for:

- start up and close down of the Council's servers (in case of failure of the autostart routines);
- back-up of data (including tape cycles) for the servers;
- database restores and event logging;

should all be documented where applicable and maintained. The procedures should be subjected to version control; any changes being authorised by Management.

5.1.2. *Operational Change Control* 💻

Upgrades to information processing facilities and systems such as the Lotus Notes server, Sophos Antivirus Software and Windows NT should be performed in a controlled manner. All documentation relating to an upgrade should be provided by the supplier. All operational programs should be subject to strict change control and when the programs are changed, the previous version kept in a separate location in case of problems associated with the latest change/s.

5.1.3. *Management of Development and Live Activities* 💻 ☞

Separation is required between development, testing and live environments in order to reduce the risk of unauthorised access to and unintended changes to software and data resulting from sharing of the same computing environment.

Further requirements are that:

- a known and stable testing environment must be maintained in order to perform accurate tests and to prevent inappropriate developer access;
- rules for the transfer of software from development to live status should be defined and documented;
- development and live software should ideally run in different domains or on different processors, but where this is not possible different directories will suffice.

In respect of any third party software development activities, the above controls will need to be stated within the terms of any contract drawn up by individual Service areas in consultation with ICT Services.

5.2 System Planning and Acceptance

5.2.1. *Capacity Planning* 💻

Capacity demands on the Council’s networked services and applications should be monitored on a regular basis. Projections of future capacity requirements should be made, taking into account any new business and system requirements; in order to ensure that adequate processing power and storage are available.

Utilisation of key system resources including processors and file storage should be analysed on a regular basis. Managers of the Council’s UNIX services should identify trends in usage, particularly in relation to business applications and management information systems, in order to prevent bottlenecks in user services.

5.3 Protection Against Malicious Software

5.3.1. *Controls Against Malicious Software* 💻 ☞☺

All users of the Council’s computers must adhere to the **Acceptable Use of Electronic Services Standards** in order to reduce the risk of malicious software being introduced into the Council’s electronic working environment.

The following additional precautions should be taken to further reduce the risk of and detect the introduction of malicious software:

- installation and regular update of anti-virus detection and repair software to scan computers on the Council’s network and freestanding laptops on a routine basis;
- reviews of the software and data content of systems supporting critical business processes should be performed. Ideally the reviews ought to be undertaken every year. The presence of any unapproved files or software should be formally investigated;
- checking all incoming e-mail attachments or Internet downloads for malicious software before use;
- inclusion of virus attack recovery procedures (for all of the Council’s networked services) in the Business Continuity Plan for ICT Services;
- procedures should be in place to verify the accuracy of all security bulletins (regarding the latest viruses) received by ICT Services. All employees should be made aware of how to recognise and handle hoaxes.

5.4 Housekeeping

5.4.1. *Information Back-up* 💻 ☞

Back-up facilities should be provided to ensure that all essential business information and software can be recovered following a disaster or media failure.

Back-up and restore procedures for the Council’s mainframe and other network services should be regularly tested and checked to ensure that they are effective and can be completed within the time allotted in the Business Continuity Plan. For third party supplied applications the requirement to supply back-up and recovery procedures should be written into the appropriate contract.

Back-ups of critical business information should be performed on a daily basis. Back-ups of associated application software should be taken every time an upgrade is applied.

All back-ups should be stored in a secure remote location together with documented recovery procedures in order to prevent any damage arising from a disaster at the main site. The physical and environmental protection afforded to media at the main site should be extended to cover the remote 'back-up' site.

5.4.2. *Operator Logs* 💻

Integris should maintain an electronic copy of the IBM SYSLOG, which should be made available to appropriate Council employees.

5.5 Security of Information and Software Exchanges

5.5.1. *Security of Systems Documentation* ☞ 💻 ☺

It is possible that systems documentation, such as functional specifications, test scripts and authorisation process details, may contain **sensitive** information which should be protected in the following ways:

- the circulation list for all types of systems documentation should be kept to a minimum and authorised by the appropriate business owner;
- all hardcopy documents should be locked away when not in use;
- all systems documentation held electronically should be restricted to authorised users only and as such should be controlled eg by using file permission utilities (operating system level) or user profiles (application level).

5.5.2. *Information Agreements* ☞💻

Agreements should be established for any exchange of information between the Council and other organisations (including software escrow agreements). The security content of such an agreement should:

- reflect the sensitivity of the business information involved;
- reference management responsibilities for controlling and notifying transmission, despatch and receipt;
- reference minimum technical standards for transmission of information;
- provide details of a classification and labelling process (which compliments **Section 9 - *Asset Classification***) for confidential information, which will ensure that the information is appropriately protected;
- consider responsibilities for Data Protection and software copyright compliance;
- special controls to be considered such as cryptographic keys.

5.5.3. *Security of Electronic Mail* ☞ 💻 ☺

Electronic Mail (e-mail) is being used increasingly for the Council's business communications, due to its speed and informality of its messaging structure. This increase in business dependency makes the Council's e-mail system vulnerable to security risks such as:

- undetected, unauthorised transactions;
- misdirection of emails;
- being unable to prove the origin of sender;
- being unable to control remote user access to Council e-mail accounts.

To reduce the risks associated with widespread use of e-mail the following controls and procedures should be complied with:

- Virus protection software should be in place to protect the e-mail network;
- Any messaging which cannot be authenticated should be vetted using an appropriate method;
- Sending of defamatory e-mails or use of the email system for harassment or unauthorised purchasing is prohibited.

In addition to these stipulations employees are required to adhere to the **Acceptable Use of Electronic Services Standards** on email communications.

5.5.4. *Security of Business Transactions over the Internet* ☞ 💻 ☺

This subject area is covered by a separate Internet Acceptable Use Policy (**see Appendix B**).

5.5.5. *Security of Publicly Available Systems* 💻 ☞

Where data and other information is published electronically (and is available to the public), such as via the Council's Internet website, the following controls are required to be in place in order to protect the integrity of information:

- access to any material published by the Council must prohibit unintentional access to other Council networks (if connected to any);
- all data published must have been obtained in compliance with the Data Protection Act (1998) and not infringe the Copyright laws.

5.5.6. *Security of Other Forms of Information Exchange* ☺

Council information could be compromised if the exchange of information via voice, fax or video communications is intercepted by unauthorised users.

Alternatively, the compromise of information could occur as a result of lack of employee awareness, policy or procedures on the use of such facilities. eg being overheard on a mobile phone in a public place.

Consequently employees are expected to observe the following when using voice, fax or video communications:

- when making phone calls which reveal sensitive information employees should:
    - be careful that there is not anyone in the immediate vicinity who could overhear or intercept the call, particularly when using mobile phones;
    - be wary of who might be listening in at the recipients end;
    - be aware that wiretapping and other forms of eavesdropping through physical access to the phone handset may occur;
- confidential conversations should not be conducted in public places, open offices or meeting places with thin walls wherever possible;
- messages containing sensitive information should not be left on answering machines since they may be replayed by unauthorised persons;
- prior to sending documents and messages out, the number dialled should be rechecked because of the implications to the Council of information being sent to the wrong number either by misdialling or from using the wrong stored number.

6. Systems Development & Maintenance

The design and implementation of the business processes to support an application or service can be crucial for security.

Therefore it is mandatory for all Service areas to identify, document and achieve ‘sign-off’ of all security requirements prior to commencement of the development stage in a project.

A further argument for this approach is that it is significantly cheaper to implement and maintain security controls introduced at the analysis and design stage, rather than during or post implementation.

In order to ensure that this occurs, the following controls and procedures should be applied as soon as possible after project initiation:

6.1 Security Requirements of Systems

6.1.1. *Security Requirements Analysis & Specification* ☞

Any statement of business requirements either for new systems, enhancements to existing systems or for commercial ‘off-the-shelf’ packages should contain details of all automated controls to be incorporated into the system; together with supporting manual ones.

All requirements should reflect the business value of the information involved and the potential business damage resulting from a breach in systems security. This is achieved by subjecting the requirements to a risk analysis.

6.1.2. *Validation Rules for Data Input* 💻 ☞

Validation should be performed on all data being input, either on-line or via a batch run job. This is in order to ensure the integrity of data on the Council’s databases and to conform to the Data Protection Act (1998).

Where possible, checks should be performed on the following types of data:
- customer reference numbers;
- names and addresses;
- financial figures;
- reference tables.

Automated checks which should be included in the security requirements specification (SRS) are:
- missing or incomplete data;
- entry of out of range values;
- entry of foreign characters in data fields;
- entry of values exceeding upper/lower data limits.

Appropriate validation error messages to be output to the screen for on-line transactions, together with outline processes for handling rejected data processed via batch runs, should also be specified in the SRS.

6.1.3. *Control of Batch Processing & Output* 💻 ☞

Procedures to be specified in the SRS to protect the integrity of data being processed in batch are:

- controls to prevent batch programs running in the wrong order or running after failure of prior processing;
- controls to ensure that the correct batch programs are kicked off following failures, thus ensuring correct processing of data;
- batch controls to reconcile data balances following transaction updates;
- reconciliation control counts to ensure processing of all data;
- validation of system-generated data (such as invoices or management information reports via manual checking);
- definition of sufficient reporting data so that the user can determine the accuracy, completeness and classification of information and make corrections where necessary.

6.2 Cryptographic Controls

NOTE: 💻 ☞

As the Councils' need to conduct business via the Internet increases, the wider use of controls such as data encryption and digital signatures will need to be addressed.

This note has been incorporated into the Security Policy in an attempt to reflect the importance of these types of controls when conducting business beyond the Council's internal boundaries.

To date data encryption is only performed on network traffic containing passwords.

Where a new application is being developed for/by the Council, there is a requirement for all passwords (usually entered via a log-on screen) to be encrypted.

6.3 Security in Systems Development and Testing Processes

6.3.1. *Change Control Procedures* 💻 ☞

Formal change control procedures should be enforced in order to minimise the corruption of information systems and ensure successful development projects. Without any change management in place, managers would have little or no control over the products their projects are producing. A standard approach to change control should be adopted by all Service areas and include:

- defining and maintaining agreed authorisation levels;
- ensuring changes are submitted by authorised users on a standardised form;
- performing an assessment of the impact of the proposed change(s) on:
  - the application involved;
  - logical security controls;
  - systems integrity procedures;
- identifying all computer software, database entities and attributes and screen templates that require amendment;
- obtaining formal approval for detailed proposals before work commences;

- maintaining a record of all change requests;
- maintaining version control over all software changes;
- ensuring that the user responsible for the area requiring change signs-off the change prior to implementation;
- ensuring that any implementation causes minimal disruption to Council services;
- ensuring that all systems documentation, user guides and user procedures associated with a change, are updated upon its implementation and that previous versions are archived;
- ensuring that testing environments, for new software are kept separate from both development and live environments in order to protect information and software already in operation.

NOTE:
For the above purposes a change request is the means by which a change is requested for an item in a system. Items may vary widely in size, complexity and type ranging from a complete system including all hardware, software and documentation to an algorithm shared by several programs.

6.3.2. *Outsourced Software Development and Managing Change* ☞ 💻

Where software is developed for the Council by a third party supplier, the following technical aspects need to be addressed and documented (included in the contract):

- how many licences will be required, who is to own the source code and the intellectual property rights;
- who is to be responsible for performing quality checks and how they are to be executed;
- rights of access in order for management to examine the quality and accuracy of development and associated work;
- requirements for coding standards during development;
- virus checks to be performed on code prior to implementation;
- training requirements for the operation or use of new systems.

Modifications post implementation should be avoided unless essential and in any case the following guidelines should be adopted prior to modifying either functions, the database structure, screen design or operational code:

- A full impact analysis should be performed to assess the risks to the existing code and the impact if the Council becomes responsible for the future maintenance of the software as a result of changes.
- Obtain the consent of the vendor (if the source code has not been purchased).
- If changes are unavoidable, the original software should be retained and the changes applied to a clearly identified copy. All changes should be fully tested and documented so that they can be reapplied if necessary to future software upgrades provided by the vendor.

6.3.3. *Systems Acceptance* 💻 ☞

Prior to acceptance of any new information systems and upgrades (whether developed in-house or by a third party); acceptance criteria and a suitable set of system tests should be established and proven.

In documenting the acceptance criteria, managers should ensure the following areas have been addressed:

- performance and capacity requirements;
- recovery from errors, associated restart procedures and business continuity plans;
- procedures to ensure the new system conforms to the Council's security standards;
- procedures to ensure that installation of the new system will not adversely affect existing systems, particularly at peak processing times.

6.4 Security of Systems Files

6.4.1. *Control of Operational Software* 💻

To minimise the risk of corruption to the operating systems when implementing new software, the following controls should be applied:

- 'Operational' program libraries should only be updated by the nominated librarian upon appropriate management authorisation.
- Executable code should not be implemented on a 'live' operating system until successful testing and user acceptance has been completed. Also, the corresponding program source libraries should have been updated.
- Where segregation of operational duties cannot be achieved, an audit trail of all updates to operational program libraries should be maintained. Audit trail listings should be produced on a monthly basis and retained for a period as determined by Internal Audit.
- Externally supplied operational software should be maintained at a level which is supported by the supplier.
- Software patches can be used to help remove or reduce security weaknesses.
- Access to operational software should only be given to suppliers for support purposes when absolutely necessary and with prior management approval. Where approval has been given, suppliers' activities should be continuously monitored.

6.4.2. *Protection of System Test Data* 💻 ☞

System/acceptance testing usually requires substantial volumes of test data.

In order that testing may be conducted in a secure manner:

- the use of 'copied live data' which may include personal and confidential details should be avoided;
- access to the test environment should be controlled by assigning individual test user IDs;
- authorisation should be obtained each time operational functions/information are copied to a test system;
- operational information should be deleted following successful completion of all testing activities.

6.4.3. *Access Control to Program Source Libraries* 💻

In order to reduce the potential for corruption of programs in the 'live' or development environments, strict control should be maintained over access to program source libraries as follows:

- program source code should not be held in operational program libraries;
- a configuration librarian should be nominated for each application. They should be responsible for updating program source libraries and issuing source code to programmers, upon authorisation from the Development Services Manager for that particular application. Emergency procedures should be identified and documented for instances where amendments are made to 'live' code out of office hours;
- any maintenance and copying of code from program source libraries should be subject to strict change control procedures (detailed in **Section 6.3 1 - *Change Control procedures***);
- ICT Services support staff should not have unrestricted access to program source libraries;
- all hardcopy program listings should be locked away (preferably in a fireproof safe) when not in use;
- where possible an audit trail should be maintained of all user accesses to program source libraries. This control applies to existing and new applications;
- old versions of source programs (except the one previous to the 'live' version) should be archived together with details of the dates and times when they were last live together with all supporting software, job control, data definitions and procedures.

7. Personnel Security

Security responsibilities should be addressed at the following stages in the employment lifecycle:

- during recruitment;
- whilst drawing up a contract;
- during a person's employment;
- on the termination of employment.

To reduce risks the following steps must be taken in relation to both permanent and temporary appointments.

More specifically in order to reduce the risks of human error, fraud and theft the following controls should be invoked:

7.1 Recruitment

7.1.1. *Resourcing & Job Definition* ☞

The following verification checks should be performed in respect of permanent, contract, temporary and casual employees at the time of job application:

- ensure that two satisfactory job references are obtained for any shortlisted candidate prior to any appointment being confirmed. One reference must be in respect of the employee's current employer (or most recent employer if unemployed). In the case of a school/college leaver one reference must be from the relevant school/college;
- every effort must be made to ensure satisfactory references have been received prior to an employee starting work;
- seek evidence of claimed academic/professional qualifications;
- for all posts covered by the CRB[2] disclosure the applicants identity should be validated by viewing one item from list A and two item from list B
    - A. current passport or new style UK driving licence or full birth certificate
    - B. address related evidence e.g. recent utility bill, bank statement

Where a job involves handling large volumes of cash, processing electronic financial transactions or handling information which is highly confidential; advice should be sought from Internal Audit on whether a credit check should be performed during the recruitment stage.

Where agency staffs are recruited the Service areas concerned must ensure that the contractual terms with the agency include the requirement to check references, qualifications and, where appropriate the credit worthiness of the individual, if the job involves significant cash handling or financial transactions.

[2] Criminal Records Bureau

The Council uses the CRB disclosure service to help assess the suitability of applicants for posts linked to children or vulnerable adults. Full details of the use of this service and the appropriate procedures are available from Personnel. A copy of the policy statement on the secure storage, handling, use, retention and disposal of any disclosure information collected is attached at **Appendix F.**

7.1.2. *Confidentiality Agreements* ☞

The Council's Code of Conduct must be brought to the attention of all newly appointed employees and referred to in their conditions of service. Within the Code is a requirement that those employees handling confidential and sensitive information must not use that information for their own personal advantage or for the advantage of any person known to them; nor must it be passed to anyone not entitled to receive it.

Confidentiality agreements should be reviewed when there are changes to terms of employment or contract, particularly when employees or contractors are leaving the Council.

Prior to a change of duties or an employee leaving, line managers should ensure that:

- the employee is informed in writing that he/she continues to be bound by the confidentiality agreement contained within the Council's Code of Conduct;
- all user IDs are removed to deny access;
- the employee's name is removed from any distribution lists;
- entry tags must be given up by those leaving the Council's employment (and any contractors who have been issued with them). Those responsible for controlling access to the premises must be informed of the employee/contractor's end date, thus preventing future entry;
- all Council property is returned e.g. keys, passes, authorisation and identity cards and any equipment or materials which belong to the Council. The leaver's checklist should ensure that this is fully complied with.

7.1.3. *Terms & Conditions of Employment* ☞

Where appropriate the terms and conditions of employment should state the employee's responsibility for information security and the action to be taken if the employee disregards security requirements. In the case of home workers, the terms and conditions of employment should state that these responsibilities are extended outside of the Council's premises and beyond normal working hours.

7.2 User Training

7.2.1. *Information Security Training* ☞

To ensure users are equipped to support the Council's Security Policy in the course of their normal work, all users should receive appropriate training.

This should take the form of:

- briefing sessions aimed at raising user awareness on information security threats to the Council;

- practical training in the correct use of information processing facilities and should be complemented by regular updates to Council policies and procedures.

7.3 Security Incidents and Malfunctions

7.3.1.*Security Incident Management Procedures* ☞

Incident management responsibilities and procedures should be determined by the Information Governance Officer, in order to ensure a quick, effective response to security incidents. A full copy of the procedures to be followed in the event of a security incident can be found at **Appendix G**. The procedures should be invoked for security incidents, such as systems failures and denials of service, which ICT Services cannot attribute to anything other than a suspected security breach or errors resulting from incomplete or inaccurate business data and breaches of confidentiality.

Audit trails and other information available should be collected and secured, to be used for:

- internal problem analysis;
- use as evidence in relation to a potential breach of contract, breach of regulatory requirement, computer misuse or breach of Data Protection legislation;
- negotiating for compensation from software and service suppliers.

7.3.2. *Disciplinary Process* ☞

A general principle to be established in respect of security is that every computer or information user is required to accept responsibility for their actions. Any breach of security rules traced to any user(s), whether through deliberate decision or negligence on their part, will be attributed to those users who will then be held accountable for the breach.

Such consequences may lead to disciplinary action against the individual(s) involved through the established disciplinary procedures.

8. Physical & Environmental Security

All Council facilities supporting critical or sensitive business activities should be housed in secure areas.

Such facilities should be physically protected from unauthorised access, damage and interference. They should be sited in secure areas, protected by a defined security perimeter, with appropriate entry controls and security barriers.

8.1 Secure Areas

8.1.1. *Physical Security Perimeter & Entry Controls* ☞

The Council's premises can be protected through implementation of a series of strategically located barriers. The requirements and siting of each physical barrier should depend on the value of the assets and services to be protected, as well as the associated security risks.

Important or particularly sensitive areas need to be protected by locks with codes which can be changed periodically.

Where an area is designated as secure e.g. a computer operations room or a locked room containing safes, or rooms inside a physical security perimeter:

- visitors should be supervised, required to wear visible authorised identification, record their date/time of entry/departure and person(s) being visited;
- access to sensitive information should be controlled and restricted to authorised persons only;
- the design of the secure area should take into account the possibility of damage from fire, flood, explosion and other disasters. It should also consider relevant health and safety regulations;
- support functions and equipment eg fax machines and printers, should be sited appropriately to avoid demands for access which could compromise confidential information;
- doors and windows should be locked when unattended and external protection should be considered for windows at ground level;
- suitable intruder detection systems should be installed to cover all external doors and accessible windows. The systems should be installed to professional standards and regularly tested;
- information processing facilities managed by the Council should be physically separated from those managed by third parties;
- access to secure areas by all third party support services personnel should be permitted only when access is required for maintenance work;
- contingency equipment and back-up media should be located at a safe distance to avoid damage resulting from a disaster at the Shirehall.

8.2 Equipment Security

8.2.1. *Equipment Siting and Protection* ☞

All equipment should be sited or protected to reduce the risks from threats such as: theft, fire, explosives, smoke, flooding, interference of electrical supplies and chemical effects.

Specifically:

- all computer terminals and other information storage facilities handling sensitive data, should be positioned away from windows where possible, to reduce the risk of being overlooked during use;
- computer environments including temperature, humidity and power supply quality should be monitored where necessary. This will help to identify conditions which may adversely affect the operation of the computer equipment, to enable any corrective action to be taken. It should always be carried out in accordance with manufacturer's recommendations.

8.2.2. *Power Supplies* ☞

All services and equipment should be suitably protected from power failures and other electrical anomalies. A suitable electricity supply should be provided that conforms to the equipment manufacturer's specifications.

An uninterruptible power supply (UPS) to support orderly close down or continuous running, is recommended as a minimum requirement for equipment supporting critical services. Contingency plans should cover the action to be taken on failure of the UPS and regular checking of equipment to ensure it has adequate capacity.

8.2.3. *Cabling Security* 💻

Power and telecommunications cabling carrying data or supporting Council services should be protected from interception or damage.

Specifically, network cabling should be protected from unauthorised interception or damage by using conduits or by avoiding routes through public areas.

Where wireless networking is in use, encryption of data is compulsory.

8.2.4. *Equipment Maintenance* 💻 ☞

On-going maintenance arrangements (defining level of maintenance and minimum levels of performance) should be the subject of contractual agreement.

If any equipment doesn't need to be maintained (as it may be cheaper to replace it) the decision process should include an impact analysis of the loss of availability.

A record of faults or suspected faults should be maintained by the ICT Services Helpdesk.

Only approved systems engineers should be allowed access to hardware or software. Where possible, systems engineers should be escorted and supervised while on site.

The systems engineer should if possible, be escorted in and out of the building and the user, or a representative of the user, should be present during the maintenance or repair operation.

Where possible, diagnostic tools for use by suppliers' employees should be obtained from the supplier and kept on site for use by systems engineers as necessary. As these disks may contain powerful software, such disks should be kept securely for use only by authorised employees.

8.2.5. *Security of Equipment Off-Premises* ☺ ☞

Information processing equipment, data or software should not be used off-site without documented management authorisation. Information processing equipment includes items such as personal computers, organisers (PDAs) and mobile phones.

The following security guidelines must be adhered to for all equipment taken off-site:

- it should not be left unattended in public places;
- manufacturer's instructions for protecting equipment should be observed at all times;
- where it is necessary to transport sensitive or personal data in this manner, data encryption must be in-place.

8.2.6. *Secure Disposal of Equipment* ☞ 💻 ☺

Where equipment has been used to process personal data under the Data Protection Act (1998) or 'in confidence' data, then any storage media should be disposed of only after reliable precautions have been taken to destroy the data.

Types of storage media housing data include:

- hardcopy documents/reports;
- magnetic tapes;
- removable disks or cassettes;
- microfiche;
- dictaphone;
- fax machines;
- answering machines;
- organiser /PDA;
- hard-drive;
- CD-ROM.

Procedures for disposal must be documented. Disposal of confidential items should be logged in order to maintain an audit trail.

Disks should be degaussed[3] where possible; otherwise the whole disk should be overwritten with randomly generated characters using software designed for this purpose. If a hard disk cannot be overwritten it should be destroyed.

[3] Degaussing a magnetic storage medium is a process to remove all the data stored on it.

8.3 General Controls

8.3.1. *Clear Desk & Clear Screen Policy* ☺

Information left out on desks is likely to be damaged or destroyed in the event of a disaster such as a fire, flood or explosion. Therefore, all confidential information and removable storage media should be removed from desk surfaces when not in use, particularly prior to employees' departure from Council premises each evening.

Additionally, the following guidelines should also be adhered to:

- sensitive or critical business information should be locked away, preferably in a fire-resistant safe or cabinet when not required;
- computer terminals should not be left logged on when unattended unless they save a password protected screensaver activated;
- sensitive or classified information when printed should be cleared from printers immediately.

8.3.2. *Removal of Property* ☞ ☺

All equipment information or software removed from site should be logged out and back in when returned. Spot checks will be undertaken to detect any unauthorised removal of property. Individuals will be notified that spot checks will take place.

9. Asset Classification

An organisation needs to be able to identify its assets together with the relative value and importance associated with each for a number of reasons:

- in order to provide levels of protection commensurate with the value and importance of the assets;
- for health and safety reasons;
- for the purposes of insurance or financial asset management.

The process of compiling an asset inventory is an important aspect of risk management.

9.1 Accountability for Assets

9.1.1. *Inventory of Assets* ☞

Managers within each Service area are responsible for drawing up an inventory of assets associated with each information system owned by them. This task should be approached in a standardised manner across service areas (see **Appendix D** for asset examples and suggested inventory contents).

In order to provide a suitable level of protection against theft in respect of the Council's assets; all physical assets (see **Appendix D**) should be labelled in an appropriate fashion.

9.2 Information Classification

9.2.1. *Classification Guidelines & Information Labelling* ☞

Organisations are increasingly using a classification to indicate the level of sensitivity of information contained within a message, such as PROTECT, RESTRICTED or NHS-CONFIDENTIAL.

When receiving information that is classified, users are responsible for ensuring the usage of the information is in accordance with the instructions of person/organisation providing the information.

9.2.2. *Information Labelling & Handling* ☞

When creating or sending information via electronic services, the Council's 'Guidance for handling personal or sensitive information' must be followed.

The procedures should apply to all types of information processing activity eg copying, archiving, transmission by e-mail, post or fax, transmission by mobile phone, voicemail and answering machine, printing and disposal.

9.2.3. *Security of Media in Transit* ☞

In order to safeguard information stored on media which is in transit:

- only reliable transport services should be used. A list of preferred couriers should be compiled and maintained;
- procedures for checking a courier’s identity should be implemented;
- packaging of data should be sufficient to protect it from physical damage;
- special controls such as use of locked containers, delivery by hand and tamper evident packaging should be used to further protect sensitive information from unauthorised disclosure.

10. Business Continuity Management

Business continuity management should be a controlled process aimed at reducing the disruption to business services (caused by disasters and security failures) to an acceptable level. Essentially the process is made up of four key stages:

- risk analysis;
- impact analysis;
- specification (via a Business Continuity Plan (BCP)) and implementation of controls aimed at reducing the identified risks;
- testing, maintaining and re-assessing BCPs.

Controls for each of these key stages are detailed in this section.

10.1 Aspects of Business Continuity Management

10.1.1. *Risk Analysis* ☞

Business continuity within the Council should begin with:

- each Service area identifying, valuing and documenting their assets by means of an asset inventory (**see Section 9.1 *Accountability for Assets***);
- subsequent identification of events that can cause interruptions to business processes (known as ‘threats’). The threats should then be linked to one or more assets in order to prioritise them by means of allocation of a risk rating;
- all assets with the same object class (eg Hewlett Packard printer in room 1 and Epson Printer in room 4 are both individual assets but their object class is the same i.e. printer) and risk rating can be grouped together and managed by reference to the group only.

Risk analysis should be approached by all Service areas in the same manner. Thus a standard risk analysis methodology and tool should be adopted by all.

When applying risk ratings, words rather than numbers should be used for a scale, since words are more meaningful.

All risks should be periodically reassessed by nominated officers within each Service area.

10.1.2. *Impact Analysis* ☞

Following the analysis of risks, each Service area should consider and document the impact of each of the threats (specified during the risk analysis) in terms of:

- breach of confidentiality;
- non-conformance with statutory legislation;
- negative effect on the Council’s reputation;
- personal safety;
- financial losses;
- disruption to Council services.

Both the risk and impact analyses should be undertaken with full involvement of the ‘Business Owner’ of each asset/asset group.

10.1.3. *Specification of a Business Continuity Plan* ☞ 💻

Plans should be developed by each Service area, to aid the maintenance or recovery of business operations in the required timescales, following interruptions to or failure of critical business processes. Once the plans have been approved, copies should be made and the originals stored in a fireproof container/room off-site.

Each BCP should address the following:

- all procedures to be performed in the event of a major failure;
- required timescales specified where appropriate;
- commitments to external organisations via service level agreements or other contracts;
- education of employees in emergency procedures including crisis management;
- testing and updating of the plans.

10.1.4. *Testing Maintaining and Re-assessing Business Continuity Plans* ☞ 💻

BCPs should be tested and updated regularly, eg yearly, thus ensuring that they are up-to-date and effective.

In order to test that recovery procedures are viable in real life situations a test plan should be drawn up for each BCP outlining the testing strategy to be adopted in the recovery of services.

It should include the following detail:

- tests covering various scenarios eg the occurrence of a further disaster during recovery procedures;
- tests to ensure the integrity of information systems;
- tests for running business processes in parallel with recovery operations away from the main site.

During any disaster recovery testing, services for which a recovery timescale has been specified should be restored within the limit specified in the BCP.

Procedures should be included in the Councils change management programme to ensure that any changes to business arrangements such as changes in:

- personnel;
- personnel details;
- business strategy;
- legislation;
- locations;
- facilities;
- business processes;
- risk,

are incorporated into a BCP as necessary, using the appropriate version control procedures.
Responsibility should be assigned for conducting regular reviews of each BCP.

11. Compliance

To ensure compliance with criminal and civil law, legislatory, contractual and security requirements; all relevant restrictions should be explicitly defined for each information system and controls implemented to support them.

11.1 Compliance with Legal Requirements

11.1.1. *Software Copyright* 💻☞☺

Proprietary software is usually supplied under the terms of a licence agreement that limits their use to specified machines and copying for the purposes of back-up only.

All users are advised not to contravene the agreement without the copyright owner's written authority.

The following controls should be implemented to ensure users compliance to the terms of the licence agreement:

- evidence retained of ownership of licences, master disks and manuals;
- utilities for ensuring that the maximum number of users permitted is not exceeded, should be switched on where the functionality exists to do so;
- random checks should be carried out by the Information Governance Officer to ensure that only authorised software and licensed products are installed on user's machines.

11.1.2. *Retention of Records* ☞ 💻

Some records held by the Council such as Tax and VAT details; need to be securely retained to meet with statutory or regulatory enquiries. Responsibility should be established for producing an archive and data retrieval policy in order for the Council to meet the necessary requirements on this subject.

The policy should provide controls to ensure:

- records to be used as evidence that the Council operates within statutory or regulatory rules are securely retained;
- adequate defence against potential civil or criminal action;
- that the financial status of the Council can be confirmed to fundholders and auditors;
- that all record types for data which the Council holds have been allocated a suitable retention period and type of storage media together with suitable methods of protection against degradation and falsification;
- any related cryptographic keys associated with archived data or digital signatures are kept securely;
- that required data can be retrieved readily and in an acceptable format when required, either by a user for information or by a court of law.

11.1.3. *Prevention of Misuse of Information Processing Facilities* ☞ 💻

Procedures for appropriate use of Council e-mail, Internet and Intranet systems are documented in the ‘**Acceptable Use of Electronic Services Standards’**, which is available on the Council’s Intranet site.

All user activities which adhere to these guidelines will be considered as ‘authorised’.

Any activity which breaches this ‘Code of Practice’ and for which an employee has failed to obtain written authorisation for; will be considered as improper use of facilities and may result in the employee(s) responsible, facing disciplinary action.

At network log-on a warning message should be displayed on the screen to the effect of:

“**The programs and data held on this system are the property of Shropshire Council and are lawfully available to authorised users for authorised Council purposes only. Access to any data or program must be authorised by the Council.**

It is a criminal offence to secure unauthorised access to any program or data, or make any unauthorised modification to the contents of this computer system.

Offenders are liable to criminal prosecution.

IF YOU ARE NOT AN AUTHORISED USER
DISCONNECT IMMEDIATELY

(**For further advice please contact ICT Services Helpdesk on Ext: 2200**)

11.1.4. *Data Protection & Privacy of Personal Information* ☞☺

Compliance with Data Protection legislation requires appropriate management structure and control. The Council’s Data Protection Officer (DPO) should provide the necessary guidance to managers and other users on their individual responsibilities and the specific procedures that should be followed.

It is the responsibility of the ‘Information Asset Owner’ appointed for each application within a Service area to keep the DPO informed about any proposals to keep personal information in a structured file and to ensure they themselves are clear as to their obligations under the relevant legislation in terms of confidentiality, integrity and availability of the data.

11.2 Compliance with the Security Policy ☞

Managers within each Service area are responsible for ensuring:

- that security procedures within their area of responsibility are carried out correctly;
- regular reviews of their information systems are conducted in order to check for compliance with the Council's Security Policy. This can partly be achieved through penetration testing conducted by an 'unbiased party'.

Appendix A

Glossary

Access Control

A set of procedures performed by hardware, software and administrators to monitor access, identify users requesting access, record access attempts and grant or deny access.

Audit Trail

In computer systems it is a chronological record of the following:
-when users log in;
-how long they are engaged in various activities;
-what they are doing;
-whether any actual or attempted security violations occurred.

Authentication

The process of establishing the legitimacy of a node or user before allowing access to requested information.
During the process, the user enters a name or account number (identification) and password (authentication).

Authorisation

The granting of rights including the granting of access based on access rights.

Availability

Ensuring that information and critical services are available to users when required.
Sometimes calculated as the percentage of time that a system can be used for productive work.

Business Critical Systems

Vital software needed to run the organisation whether custom-written or commercially packaged applications such as accounting, finance, human resources etc.

Business Owner

Individuals, section or department having responsibility for specified information asset(s) and for the maintenance of appropriate security measures

Confidentiality

Protection of sensitive information from unauthorised disclosure

Data

Information. Any series of bit, characters or objects that has meaning. Data is stored and transmitted by computers.

APPENDIX A

Glossary

Digital Signature

Provides proof of authorship of an e-mail. It is generated for each message using fingerprint of message content and a private key. Only the corresponding public key can decrypt it

Encryption

The process of taking information and applying a mathematical algorithm to scramble it, so that only the intended recipient (who holds the key to unscrambling the information) can read it.

Impact

An assessment of the consequences to the Council or information system components of the occurrence of a particular security breach in terms of financial loss or embarrassment.

Integrity

Safeguarding the accuracy and completeness of information and software.

Remote Access

The hook-up of a remote computing device via communications lines such as ordinary phone lines or WANS (Wide Area Networks) to access network applications and information.

Server

A machine whose sole purpose is to supply data so that other machines can use it.

User

Any person who interacts directly with a computer system or uses Information as part of their duties.

User ID

A unique character string that identifies an individual user.

APPENDIX B

INTERNET ACCEPTABLE USE POLICY

Please note that this section has been superseded by the ‘Acceptable Use of Electronic Services’ Standards.

Appendix C

Incident Classification Table

Incident Level	Degree of Embarrassment to the Council	Disruption to Services	Effect on Personal Safety of Staff	Degree of Breach in Confidentiality or Integrity of Data	Financial Damage Resulting From Legal Action	Financial Loss Resulting From Disruption to Services
Insignificant	Contained within Department	Little if any effect on services	Minor injury to individual	Isolated incidences of incorrect data on a database	Civil suit < £10,000 damages	Up to £10,000
Minor	Contained within the Council	Minor disruption to a few services for up to 2 hours	Minor injury to several individuals	Isolated personal detail revealed or several incidences of incorrect data on a database	Civil suit < £10,000 damages Small fine <£10,000	Between £10,001 and £100,000
Significant	Local public or Press interested or public questions raised	Major disruption to a service for several hours	Major injury to an individual (but not death)	Several instances of personal details being revealed or small amounts of incorrect data on several databases	Large fine > £10,000	Between £101,001 and £500,000
Major	National public or press aware of incident or incidents attracts Commons debate	Major disruption to all services for a day	Major injury to several people or death of an individual	A large number of personal details being revealed or large amounts of incorrect data on many systems	Custodial sentence imposed	Between £501,001 and £1 million
Disastrous	Relentless Press attention or a total loss of public confidence in Local Government	All services are unavailable for several days or longer	Death of several people	All personal details being revealed or all data on all systems incorrect	Multiple civil or criminal suits	In excess of £1 million

Appendix D

Asset Types

Asset Type	Examples
Information	Databases, data files, system documentation, user manuals, training course material, operational procedure guides, business continuity plans and archived information
Software	Application software, systems utility software, case tools and graphics
Physical	Processors, monitors, laptops, modems, routers, fax machines, answering machines, magnetic media, power supplies, Air-conditioning units furniture, and accommodation
Services	All computing and communications services and provision of power

Suggested Asset Attributes to be Included on Inventories

Asset Type
Asset description (Including identifying marks where applicable such as make, model, serial number and software version)
Value
Location
Business owner

Appendix E

Matrix of responsibilities under the Information Security Policy

	IT Specialists 💻	**Senior Officers within all Service areas** ☞	**All Users** ☺
Sections 1 -3 - Introduction, Scope & Objectives			
	✓	✓	✓
Section 4 - System Access Control			
4.1.1 User registration & review of user access rights	✓	✓	
4.1.2 Third party access	✓	✓	
4.1.3 Privilege management	✓	✓	
4.1.4 User password management	✓	✓	
4.1.5 Logical password management	✓		
4.1.6 User responsibilities (password management)			✓
4.1.7 User responsibilities for access control of unattended equipment			✓
4.1.8 User responsibilities - access control of unattended off-site equipment			✓
4.2.1 Monitoring of application access	✓		
4.2.2 Clock synchronisation	✓		
4.3.1 User and node authentication for external connections	✓		
4.3.2 Network routing controls for third party access	✓		
4.3.3 Operating system access control	✓		
4.3.4 Internet access control	✓	✓	
Section 5 - Communications & Operations Management			
5.1.1 Documented operating procedures	✓		
5.1.2 Operational change control	✓		
5.1.3 Management of development & live activities	✓	✓	
5.2.1 Capacity planning	✓		
5.3.1 Controls against malicious software	✓	✓	✓
5.4.1 Information back-up	✓	✓	
5.4.2 Operator logs	✓		
5.5.1 Security of systems documentation	✓	✓	✓
5.5.2 Information agreements	✓	✓	
5.5.3 Security of electronic mail	✓	✓	✓
5.5.4 Security of business transactions over the Internet	✓	✓	✓
5.5.5 Security of publicly available systems	✓	✓	
5.5.6 Security of other forms of information exchange			✓

Matrix of responsibilities under the Information Security Policy

	IT Specialists 💻	**Senior Officers within all Service areas** ☞	**All Users** ☺
Section 6 - Systems Development & Maintenance			
6.1.1 Security requirements analysis & specification		✓	
6.1.2 Validation rules for data input	✓	✓	
6.1.3 Control of batch processing & output	✓	✓	
6.2 Cryptographic controls	✓	✓	
6.3.1 Change control procedures	✓	✓	
6.3.2 Outsourced software development & managing change	✓	✓	
6.3.3 Systems acceptance	✓	✓	
6.4.1 Control of operational software	✓		
6.4.2 Protection of test data	✓	✓	
6.4.3 Access control to program source libraries	✓		
Section 7 - Personnel security			
7.1.1 Resorting & job definition		✓	
7.1.2 Confidentiality agreements		✓	
7.1.3 Terms & conditions of employment		✓	
7.2.1 Information security training		✓	
7.3.1 Security incident management procedures		✓	
7.3.2 Disciplinary process		✓	✓
Section 8 - Physical & environmental security			
8.1.1 Physical security perimeter & entry controls		✓	
8.2.1 Equipment siting & protection		✓	
8.2.2 Power supplies		✓	
8.2.3 Cabling security	✓		
8.2.4 Equipment maintenance	✓	✓	
8.2.5 Security of equipment off-premises		✓	✓
8.2.6 Secure disposal of equipment	✓	✓	✓
8.3.1 Clear desk & clear screen policy			✓
8.3.2 Removal of property		✓	✓
Section 9 - Asset Classification			
9.1.1 Inventory of assets		✓	
9.2.1 Classification guidelines & information labelling		✓	
9.2.2 Information labelling & handling		✓	
9.2.3 Security of media in transit		✓	

	IT Specialists 💻	**Senior Officers within all Service areas** ☞	**All Users** ☺
Section 10 - Business Continuity Management			
10.1.1 Risk analysis		✓	
10.1.2 Impact analysis		✓	
10.1.3 Specification of a business continuity plan	✓	✓	
10.1.4 Testing maintaining and re-assessing business continuity plans	✓	✓	
Section 11 - Compliance			
11.1.1 Software copyright	✓	✓	✓
11.1.2 Retention of records	✓	✓	
11.1.3 Prevention of misuse of information processing facilities	✓	✓	
11.1.4 Data protection and privacy of personal information		✓	
11.2 Compliance with the Security Policy		✓	
Appendices			
Appendix A Glossary	✓	✓	✓
Appendix B Internet Security Policy **[superseded by Acceptable Use of Electronic Services Standards].**	✓	✓	✓
Appendix C Incident Classification	✓	✓	
Appendix D Asset Types		✓	
Appendix E Responsibility Matrix	✓	✓	✓
Appendix F Disclosure process		✓	
Appendix G Security Incident Procedures	✓	✓	✓

Appendix F

Policy Statement on the Secure Storage, Handling, Use, Retention and Disposal of Disclosure Information

General Principles

As an organisation using the CRB[4] disclosure service to help assess the suitability of applicants for positions of trust, Shropshire Council complies fully with the CRB Code of Practice regarding the correct handling, use, storage, retention and disposal of disclosures and Disclosure information. It also complies fully with its obligations under the Data Protection Act (1998) and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of disclosure information.

Storage and Access

Disclosure information is never kept on an applicant's personnel file and is always kept separately and securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

Handling

In accordance with section 124 of the Police Act (1997), disclosure information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom disclosures or disclosure information has been revealed and we recognise that it is a criminal offence to pass this information to anyone who is not entitled to receive it.

Usage

Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Retention

Once a recruitment (or other relevant) decision has been made, we do not keep disclosure information for any longer than is absolutely necessary. This is generally for a period of up to 6 months, to allow for the consideration and resolution of any disputes or complaints. If in very exceptional circumstances, it is considered necessary to keep disclosure information for longer than 6 months, we will consult the CRB about this and will give full consideration to the Data Protection Act (1998) and Human Rights Act (2000) before doing so. Throughout this time, the usual conditions regarding safe storage and strictly controlled access will prevail.

Disposal

Once the retention period has elapsed, we will ensure that any disclosure information is immediately suitably destroyed by secure means, i.e. by shredding, pulping or burning. While awaiting destruction, disclosure information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack). We will not keep any photocopy or other image of the disclosure or any copy of representation of the

[4] Criminal Records Bureau

contents of a disclosure. However, notwithstanding the above, we may keep a record of:

- the date of issue of a disclosure;
- the name of the subject;
- the type of disclosure requested;
- the position for which the disclosure was requested;
- the unique reference number of the disclosure;
- the details of the recruitment decision taken.

Acting as an Umbrella Body

Before acting as an umbrella body (one which countersigns applications and receives disclosure information on behalf of other employers or recruiting organisations), we will take all reasonable steps to ensure that they comply fully with the CRB Code of Practice.

We will also take all reasonable steps to satisfy ourselves that they will handle, use, store, retain and dispose of disclosure information in full compliance with the CRB Code and in full accordance with this Policy. We will also ensure that any body or individual, at whose request applications for disclosure are countersigned, has such a written policy, and if necessary, will provide a model policy for that body or individual to use or adapt for this purpose.

Appendix G

Security Incident Management Procedures

Policy Objective

The objective of this Policy is to minimise the damage from security incidents and malfunctions and to monitor and learn from such incidents.

Responsibilities

Incident management responsibilities and procedures should be determined by the Information Governance Officer in order to ensure a quick, effective response to security incidents.

All Users

The procedures should be invoked for security incidents such as systems failures and denials of service which ICT Services cannot attribute to anything other than a suspected security breach or errors resulting from incomplete or inaccurate business data and breaches of confidentiality.

Audit trails and other information available should be collected and secured to be used for:

- internal problem analysis;
- use as evidence in relation to a potential breach of contract, breach of regulatory requirement, computer misuse or breach of Data Protection legislation;
- negotiating for compensation from software and service suppliers.

Fault Logging

A ‘fault’ is classified for the purposes of this Security Policy as one or more of the following:

- display of an error message to a user’s screen resulting from either;
  - an application error,
  - a database inconsistency,
  - an operating system error,
- denial of service after entry of a valid user ID/password combination;
- user has exceeded current password expiry date without having changed their password; access to network services being denied.

In the first instance all faults should be reported by users to the ICT Services Helpdesk on ext 2200.

If a problem is deemed by the Helpdesk to be related to a security incident, then it should be reported immediately to the Information Governance Officer and the appropriate user’s line manager.

All fault logs will be subjected to an independent review to ensure that the details being recorded are consistent and that faults with a status of ‘closed’ have been satisfactorily resolved.

Security Incidents

A security incident for these purposes is classified as either a fault which Helpdesk have subsequently deemed to be resulting from a security breach, or any event identified by a user that has resulted in or could result in:

- the disclosure of confidential information to any unauthorised individual;
- the integrity of the system or data being put at risk;
- the availability of the system or information being put at risk;
- an adverse impact on the Council eg:
    - embarrassment to the Council,
    - threat to personal safety or privacy of employees,
    - legal obligation or penalty,
    - financial loss,
    - disruption of activities,

A formal reporting procedure should be established and documented together with an incident response procedure, setting out the action to be taken on receipt of an incident report.

The procedures should be clearly laid down, easily understood and provided to an employee as soon as possible after commencement of employment.

Security incidents can be classified as follows:

- ***common everyday events*** - eg wrong password or user ID entered, other minor log-on violations, password;

- ***uncommon events*** - where something more unusual occurs eg foreign characters or patterns filling a screen, disappearance of system files, the presence of unaccompanied unidentified strangers in a restricted area.

Mainly as a result of human error, there are likely to be large volumes of common incidents and it will not be cost effective to log all of them individually. Therefore, wherever practical, statistics should be gathered so that unusual trends or anomalies may be detected. This gathering of information should be complemented by automatic logging of electronic user activities and on request the resultant summary report sent to the Information Governance Officer for review (see section ***4.2.1 Monitoring of Application Access*** for the minimum level of information to be logged electronically).

Uncommon incidents resulting in a breach of security are many and varied. Their severity will depend on:

- the timing and location of the incident;
- the person(s) involved;
  and possibly
- the sensitivity of the information/data involved;
- the system being used to access the data.

Any uncommon incidents should be reported immediately to the Information Governance Officer. Where any of the Council's computer networks are or could be involved in the incident, the ICT Services Manager should also be informed.

The Information Governance Officer should maintain an ‘uncommon incident’ log composed of the following information for each incident:

- a unique incident number;
- a brief title;
- Incident date;
- Person responsible for reporting the incident;
- Incident location;
- Incident classification;
- Person/department responsible for investigating incident;
- Incident resolution;
- Incident resolution date/time;
- Incident status.

All ‘uncommon incident’ logs should be kept and made immediately available for management review.

If an incident is classified as significant, major or disastrous (see B, a report should be sent immediately to the Council’s Senior Information Risk Owner (SIRO)..

An incident may need to be re-classified during the course of an investigation.

For employees reporting suspected security breaches by their own superiors, an alternative line of reporting should be provided.

These reporting lines should ensure absolute protection and confidentiality for the party reporting the incident, even in the event of a ‘false alarm’.

Disciplinary Process

A general principle to be established in respect of security is that every computer user is required to accept responsibility for their actions.

Any breach of security rules traced to any user(s), whether through deliberate decision, accident or negligence on their part, will be attributed to those users who will then be held accountable for the breach. Such consequences may lead to disciplinary action against the individual(s) involved through the established disciplinary procedures.

ARIS Service Call Examples

The below SOAP Request/Response is a complete service call to our Message broker/Middleware system named ARIS, which handles all messages to and from thrid party systems.

```
//------------------------------------------------------------------------------
// Full SOAP packet containing the SCC Request XML serialized to type String
//------------------------------------------------------------------------------

POST /ARIS/services/SOAP/SCCMessage HTTP/1.0
Content-Type: text/xml; charset=utf-8
Accept: application/soap+xml, application/dime, multipart/related, text/*
User-Agent: Axis/1.3
Host: 10.1.2.193:8081
Cache-Control: no-cache
Pragma: no-cache
SOAPAction: ""
Content-Length: 1199

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Body>

        <process soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">

                <request xsi:type="xsd:string">
        &lt;sccrequest&gt;&lt;action&gt;findAddress&lt;/action&gt;&lt;context&gt;000000001&lt;/context&gt;&lt;loglevel&gt;INFO&lt;/loglevel&
gt;&lt;parameters&gt;&lt;parameter name=&quot;address&quot;
&gt;&lt;![CDATA[&lt;address&gt;&lt;id&gt;&lt;/id&gt;&lt;name1&gt;&lt;/name1&gt;&lt;name2&gt;&lt;/name2&gt;&lt;streetnumber&gt;4&lt;/str
eetnumber&gt;&lt;street&gt;&lt;/street&gt;&lt;locality&gt;&lt;/locality&gt;&lt;town&gt;&lt;/town&gt;&lt;county&gt;&lt;/county&gt;&lt;postcode
&gt;sy25yd&lt;/postcode&gt;&lt;postaladdress&gt;&lt;/postaladdress&gt;&lt;areacode&gt;&lt;/areacode&gt;&lt;areaname&gt;&lt;/areaname&g
t;&lt;easting&gt;&lt;/easting&gt;&lt;northing&gt;&lt;/northing&gt;&lt;usage&gt;&lt;/usage&gt;&lt;name2number&gt;&lt;/name2number&gt;&lt
;/address&gt;]]&gt;&lt;/parameter&gt;&lt;/parameters&gt;&lt;/sccrequest&gt;
                </request>

        </process>
</soapenv:Body>
</soapenv:Envelope>
```

```
//-------------------------------------------------------------------------------
// The Actual SCC Request XML packet within the SOAP called above.
//
// This request is using the findAddress action which relates to locating
// an address or list of addresses based on the values you provide with the
// address xml object.
//-------------------------------------------------------------------------------

<sccrequest>

        <action>findAddress</action>
        <context>000000001</context>
        <loglevel>INFO</loglevel>
        <parameters>
                <parameter name="address" >

        <![CDATA[<address><id></id><name1></name1><name2></name2><streetnumber>4</streetnumber><street></street><locali
ty></locality><town></town><county></county><postcode>SY2
5YD</postcode><postaladdress></postaladdress><areacode></areacode><areaname></areaname><easting></easting><northing></no
rthing><usage></usage><name2number></name2number></address>]]>
                </parameter>
        </parameters>

</sccrequest>
```

// Elements within SCC Request

action = Requested service which is internally mapped to specific handlers.

context = A reference value (usually the CRM case number) with provides more specific looging.

loglevel = Value declaring at what level should looging take place within the system.

parameters = encapsulates one or more paramater values.

parameter = CDATA section which contains an XML version of an object which the specific handler (Mentioned in the ACTION event above) will understand. (This also can be a straigh String / HTML etc.)

```
//-------------------------------------------------------------------------------
// Full SOAP packet responding to the above request
//
// Returns the expected object (The address object in the case, the same as the
// object we provided above, but with the extra information added)
//-------------------------------------------------------------------------------

HTTP/1.1 200 OK
Content-Length: 1225
Date: Wed, 13 Sep 2006 15:13:45 GMT
Server: Apache-Coyote/1.1
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Body>

        <processResponse soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
                <processReturn xsi:type="xsd:string">

        &lt;sccresponse&gt;&lt;status&gt;OK&lt;/status&gt;&lt;context&gt;000000001&lt;/context&gt;&lt;message&gt;&lt;![CDATA[null]]&gt;&l
t;/message&gt;&lt;data&gt;&lt;![CDATA[&lt;addresses&gt;&lt;address&gt;&lt;id&gt;&lt;/id&gt;&lt;name1&gt;&lt;/name1&gt;&lt;name2&gt;&lt;
/name2&gt;&lt;streetnumber&gt;4&lt;/streetnumber&gt;&lt;street&gt;Longbridge
Close&lt;/street&gt;&lt;locality&gt;&lt;/locality&gt;&lt;town&gt;SHREWSBURY&lt;/town&gt;&lt;county&gt;&lt;/county&gt;&lt;postcode&gt;SY2
5YD&lt;/postcode&gt;&lt;postaladdress&gt;&lt;/postaladdress&gt;&lt;areacode&gt;&lt;/areacode&gt;&lt;areaname&gt;&lt;/areaname&gt;&lt;ea
sting&gt;&lt;/easting&gt;&lt;northing&gt;&lt;/northing&gt;&lt;usage&gt;&lt;/usage&gt;&lt;name2number&gt;&lt;/name2number&gt;&lt;/addre
ss&gt;&lt;/addresses&gt;]]&gt;&lt;/data&gt;&lt;/sccresponse&gt;
                </processReturn>
        </processResponse>
```

```
</soapenv:Body>
</soapenv:Envelope>
```

```
//-------------------------------------------------------------------------------
// The Actual SCC Response XML packet
//-------------------------------------------------------------------------------

<sccresponse>

	<status>OK</status>
	<context>000000001</context>
	<message>
		<![CDATA[null]]>
	</message>

	<data>

	<![CDATA[<addresses><address><id></id><name1></name1><name2></name2><streetnumber>4</streetnumber><street>Longbridge Close</street><locality></locality><town>SHREWSBURY</town><county></county><postcode>SY2 5YD</postcode><postaladdress></postaladdress><areacode></areacode><areaname></areaname><easting></easting><northing></northing><usage></usage><name2number></name2number></address></addresses>]]>
	</data>

</sccresponse>
```

// Elements within the SCC Response
status = A short message indicating the outcome of the requested action.
context = A reference value (usually the CRM case number) with provides more specific looging.
message = Used primarily for failure reason.
data = The response to your request. Can be anything, a XML version of an object HTML, or standard String values. etc.

```
//------------------------------------------------------------------------------
// Full SOAP request for containing the SCC Message with the action set to
// findNames
//------------------------------------------------------------------------------

POST /ARIS/services/SOAP/SCCMessage HTTP/1.0
Content-Type: text/xml; charset=utf-8
Accept: application/soap+xml, application/dime, multipart/related, text/*
User-Agent: Axis/1.3
Host: 10.1.2.193:8081
Cache-Control: no-cache
Pragma: no-cache
SOAPAction: ""
Content-Length: 1197

<?xml version="1.0" encoding="UTF-8"?>
```

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Body>

        <process soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
                <request xsi:type="xsd:string">

        &lt;sccrequest&gt;&lt;action&gt;findNames&lt;/action&gt;&lt;context&gt;000000001&lt;/context&gt;&lt;loglevel&gt;INFO&lt;/loglevel&g
t;&lt;parameters&gt;&lt;parameter name=&quot;address&quot;
&gt;&lt;![CDATA[&lt;address&gt;&lt;id&gt;&lt;/id&gt;&lt;name1&gt;&lt;/name1&gt;&lt;name2&gt;&lt;/name2&gt;&lt;streetnumber&gt;4&lt;/str
eetnumber&gt;&lt;street&gt;&lt;/street&gt;&lt;locality&gt;&lt;/locality&gt;&lt;town&gt;&lt;/town&gt;&lt;county&gt;&lt;/county&gt;&lt;postcode
&gt;sy25yd&lt;/postcode&gt;&lt;postaladdress&gt;&lt;/postaladdress&gt;&lt;areacode&gt;&lt;/areacode&gt;&lt;areaname&gt;&lt;/areaname&g
t;&lt;easting&gt;&lt;/easting&gt;&lt;northing&gt;&lt;/northing&gt;&lt;usage&gt;&lt;/usage&gt;&lt;name2number&gt;&lt;/name2number&gt;&lt
;/address&gt;]]&gt;&lt;/parameter&gt;&lt;/parameters&gt;&lt;/sccrequest&gt;
                </request>
        </process>
</soapenv:Body>
</soapenv:Envelope>
```

```
//------------------------------------------------------------------------------
// The SCC Request from above but in true XML. Notice we provice an address
// object again. Infact the same object we had returned to us in the call above
//------------------------------------------------------------------------------
<sccrequest>
        <action>findNames</action>
        <context>000000001</context>
        <loglevel>INFO</loglevel>
        <parameters>
                <parameter name="address" >
        <![CDATA[<address><id></id><name1></name1><name2></name2><streetnumber>4</streetnumber><street></street><locali
ty></locality><town></town><county></county><postcode>sy25yd</postcode><postaladdress></postaladdress><areacode></areacod
e><areaname></areaname><easting></easting><northing></northing><usage></usage><name2number></name2number></address>
]]>
                </parameter>
        </parameters>
</sccrequest>




//------------------------------------------------------------------------------
// The SCC Response this time returns a Names XML object, listing all names
// at the address provided to us in the address object
//------------------------------------------------------------------------------
<sccresponse>
        <status>OK</status>
        <context>000000001</context>
        <message>
                <![CDATA[null]]>
        </message>

        <data>

        <![CDATA[<names><name><title>Mr</title><forename>Christopher</forename><submittedForename>Christopher</submittedFor
ename><middleInitial>P</middleInitial><surname>Jones</surname><organisation></organisation></name><name><title>Mr</title><fo
rename>David</forename><submittedForename>David</submittedForename><middleInitial>R</middleInitial><surname>Jones</surname
><organisation></organisation></name><name><title>Ms</title><forename>Margaret</forename><submittedForename>Margaret</sub
mittedForename><middleInitial>J</middleInitial><surname>Jones</surname><organisation></organisation></name><name><title>Mr<
/title><forename>Steven</forename><submittedForename>Steven</submittedForename><middleInitial>A</middleInitial><surname>Jones</surname><organisation></organisation></name></names>]]>
          </data>
</sccresponse>
```

ARIS SOAP messaging specification

v1.2.5

Document history

Version	Date	Editor	Details
v1.2.0	04/02/2008	[redacted]	New document based on v1.0.5 of ARIS messaging specification
v1.2.1	06/02/2008	[redacted]	Document release
v1.2.2	07/02/2008	[redacted]	Updates to structure, changes to WSDL
v1.2.3	08/02/2008	[redacted]	Document update, changes to context
v1.2.4	11/02/2008	[redacted]	Modified response and WSDL examples
V1.2.5	18/02/2010	[redacted]	Re-branded as “Shropshire Council”

Introduction

Shropshire Council developed the ARIS messaging specification to provide a simple and generic way to pass messages into the ARIS system, without having to provide custom interfaces for handling service specific ‘hard-typed’ messages.

ARIS exposes only one SOAP entry point, so any external system wanting to communicate with ARIS must provide some configuration within the SOAP request. This allows ARIS to identify the type of message by interrogating its own configuration.

The messaging specification is a simple XML wrapper for both request and response interactions. It contains a small collection of ARIS specific elements, but also provides elements for the embedding of one or many complex messages.

The ARIS messages are named ‘**SCCRequest**’ and ‘**SCCResponse**’, which respectively handle any messages sent into ARIS and the resulting output message from ARIS.

SCCRequest

The **SCCRequest** has two logical sections that are referred to as the header elements, and the body elements.

ARIS uses the header elements for identifying system state as well as the actual action it must perform, with any embedded data in the body elements.

The body elements comprise a collection of one or more elements, with the content specified in an XML encoded character data (CDATA) section.

This provides us with the flexibility of taking hard-typed XML documents, binary data, or anything else that is required.

SCCRequest message header elements

The **SCCRequest** header elements are contained within the main **SCCRequest** element, and are loosely typed. This is to provide greater flexibility when working with different systems.

Element	Type	Mandatory	Description
action	String	**Yes**	This provides ARIS with the configuration necessary to identify the service required. This value must match a value in the ARIS configuration file. If you do not provide this value, ARIS will return a **SCCResponse** message containing error information.
context	String	No	This is a reference number related to the request. This value is used for tracing the message through the ARIS system, it is not required, but you should provide it if possible.
loglevel	String	No	This element is used exclusively for tracing problems within the ARIS system. This should be set to **INFO** unless stated otherwise. Other values allowed are **FATAL**, **ERROR**, **WARN**, **DEBUG**, but as stated should not be used unless specified otherwise.

Example SCCRequest message header extract (XML)

```
<sccrequest>

      <action>ARIS.EXAMPLE_ACTION</action>

      <context>L00000001</context>

      <loglevel>INFO</loglevel>

      ...

</sccrequest>
```

SCCRequest body elements

The body elements are composed of a single ‘**parameters**’ element which contains a collection of one or many ‘**parameter**’ elements.

Each ‘**parameter**’ element has a single mandatory attribute called ‘**name**’, the value of this attribute must be unique within the ‘**parameters**’ collection, otherwise ARIS will ignore any subsequently named parameter elements.

The value within the ‘**parameter**’ element itself can be any type of data, as long as it has been correctly XML encoded.

Example SCCRequest body extract (XML)

```
<sccrequest>

      ...

      <parameters>

            <parameter name="postcode">
                  <![CDATA[SY2 6ND]]>
            </parameter>

            <parameter name="some-xml">
                  <![CDATA[
                  &lt;Update&gt;
                        &lt;AuthorityReference&gt;
                              F0000000000003
                        &lt;/AuthorityReference&gt;
                        &lt;CaseStatus&gt;
                              Active
                        &lt;/CaseStatus&gt;
                        &lt;StatusReason&gt;
                              New
                        &lt;/StatusReason&gt;
                  &lt;/Update&gt;
                  ]]>
            </parameter>

      </parameters>

</sccrequest>
```

ARIS messaging examples

Example 1 of an SCCRequest message – Embedded XML

```
<sccrequest>
      <action>ARIS.FINDADDRESS</action>
      <context>D00003501</context>
      <loglevel>INFO</loglevel>
      <parameters>
            <parameter name="address">
                  <![CDATA[<address><id></id><name1></name1><name2>
                  </name2><streetnumber></streetnumber><street>
                  </street><locality></locality><town></town><county>
                  </county><postcode>SY26ND</postcode><postaladdress>
                  </postaladdress><areacode></areacode><areaname>
                  </areaname><easting></easting><northing></northing>
                  <usage></usage><name2number></name2number></address>
                  ]]>
            </parameter>
      </parameters>
</sccrequest>
```

Example 2 of an SCCRequest message – Multi parameter values

```
<sccrequest>
      <action>BOOKINGS.MAKEPAYMENT</action>
      <context>D00006624</context>
      <loglevel>INFO</loglevel>
      <parameters>
            <parameter name="BookingReference">
                  <![CDATA[0000001]]>
            </parameter>
            <parameter name="CostCentre">
                  <![CDATA[A1]>
            </parameter>
            <parameter name="Subjective">
                  <![CDATA[A1]]>
            </parameter>
            <parameter name="AmountBilled">
                  <![CDATA[12.78]]>
            </parameter>
            <parameter name="AmountPaid">
                  <![CDATA[12.78]]>
            </parameter>
      </parameters>
</sccrequest>
```

Example 3 of an SCCRequest message – SOAP packet

```
POST /ARIS/services/SOAP/SCCMessage HTTP/1.0
Content-Type: text/xml; charset=utf-8
Accept: application/soap+xml, application/dime, multipart/related, text/*
User-Agent: Axis/1.3
Host: 10.1.2.193:8081
Cache-Control: no-cache
Pragma: no-cache
SOAPAction: ""
Content-Length: 1199

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
      xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
      xmlns:xsd="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <soapenv:Body>
            <process soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
                  <request xsi:type="xsd:string">

      &lt;sccrequest&gt;&lt;action&gt;ARIS.FINDADDRESS&lt;/action&gt;&lt;context&gt;D00003501&lt;/context
      &gt;&lt;loglevel&gt;INFO&lt;/loglevel&gt;&lt;parameters&gt;&lt;parameter name=&quot;address&quot;
      &gt;&lt;![CDATA[&lt;address&gt;&lt;id&gt;&lt;/id&gt;&lt;name1&gt;&lt;/name1&gt;&lt;name2&gt;&lt;/na
      me2&gt;&lt;streetnumber&gt;&lt;/streetnumber&gt;&lt;street&gt;&lt;/street&gt;&lt;locality&gt;&lt;/l
      ocality&gt;&lt;town&gt;&lt;/town&gt;&lt;county&gt;&lt;/county&gt;&lt;postcode&gt;sy26nd&lt;/postcod
      e&gt;&lt;postaladdress&gt;&lt;/postaladdress&gt;&lt;areacode&gt;&lt;/areacode&gt;&lt;areaname&gt;&l
      t;/areaname&gt;&lt;easting&gt;&lt;/easting&gt;&lt;northing&gt;&lt;/northing&gt;&lt;usage&gt;&lt;/us
      age&gt;&lt;name2number&gt;&lt;/name2number&gt;&lt;/address&gt;]]&gt;&lt;/parameter&gt;&lt;/paramete
      rs&gt;&lt;/sccrequest&gt;

                  </request>
            </process>
      </soapenv:Body>
</soapenv:Envelope>
```

SCCResponse

The **SCCResponse** message is similar to the **SCCRequest** message. It contains a logical message header and body section, but only provides two body elements, instead of a collection.

SCCResponse message header elements

Element	Type	Description
status	String	This value specifies the status of the requested service/action. There are two return values currently, and this will be either **OK** or **error**.
context	String	The value within this element will be the same as the value specified in the context element in the **SCCRequest** message. This provides a consistency between the **SCCRequest** and **SCCResponse**.

SCCResponse message body elements

Element	Type	Description
data	CDATA	This element contains any expected return data. ARIS will return a value of **null** if there are no results and the **status** element is set to **OK**. If **status** is set to **error** then this will include the details on why the error occurred.
message	CDATA	This element will contain supporting data to the **data** field mentioned above, but should in most cases return a value of **null**.

Example SCCResponse messages

SUCCESS (No return data)

```
<sccresponse>
      <status>OK</status>
      <context>L00000001</context>
      <data><![CDATA[null]]></data>
      <message><![CDATA[null]]></message>
</sccresponse>
```

SUCCESS (With return data)

```
<sccresponse>

      <status>OK</status>

      <context>L00000001</context>
      <data>
            <![CDATA[<addresses><address><id></id><name1></name1><n
            ame2></name2><streetnumber>4</streetnumber><street>Long
            bridge
            Close</street><locality></locality><town>SHREWSBURY</to
            wn><county></county><postcode>SY2
            5YD</postcode><postaladdress></postaladdress><areacode>
            </areacode><areaname></areaname><easting></easting><nor
            thing></northing><usage></usage><name2number></name2num
            ber></address></addresses>]]>
      </data>
      <message><![CDATA[null]]></message>

</sccresponse>
```

FAILURE

```
<sccresponse>

      <status>error</status>
      <context>L00000001</context>
      <data>
            <![CDATA[FrameworkErrorHandler: ARIS is  unable to
            handle the following request.  Action = Test Action
            context = ArisAdapterTest. Because  unknown action
            received:  Test Action]]>
      </data>
      <message><![CDATA[null]]></message>

</sccresponse>
```

ARIS WSDL

The ARIS Web Services Description Language (WSDL) describes how a SOAP client should call the SOAP service. It provides details on the location of the service as well as the key elements.

```
<?xml version="1.0" encoding="UTF-8"?>

<wsdl:definitions targetNamespace="http://framework.scc.gov"
      xmlns:apachesoap="http://xml.apache.org/xml-soap"
      xmlns:impl="http://framework.scc.gov"
      xmlns:intf="http://framework.scc.gov"
      xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
      xmlns:wsdlsoap="http://schemas.xmlsoap.org/wsdl/soap/"
      xmlns:xsd="http://www.w3.org/2001/XMLSchema">

      <wsdl:message name="processResponse">
            <wsdl:part name="processReturn" type="soapenc:string"/>
      </wsdl:message>


      <wsdl:message name="processRequest">
            <wsdl:part name="reqs" type="soapenc:string"/>
      </wsdl:message>

      <wsdl:portType name="SCCMessage">
            <wsdl:operation name="process" parameterOrder="reqs">
                  <wsdl:input message="impl:processRequest" name="processRequest"/>
                  <wsdl:output message="impl:processResponse" name="processResponse"/>
            </wsdl:operation>
      </wsdl:portType>
      <wsdl:binding name="SCCMessageSoapBinding" type="impl:SCCMessage">

            <wsdlsoap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>

            <wsdl:operation name="process">

                  <wsdlsoap:operation soapAction=""/>

                  <wsdl:input name="processRequest">
                        <wsdlsoap:body
encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" namespace="http://framework.scc.gov"
use="encoded"/>
                  </wsdl:input>

                  <wsdl:output name="processResponse">
                        <wsdlsoap:body
                        encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
                        namespace="http://framework.scc.gov"
                        use="encoded"/>
                  </wsdl:output>

            </wsdl:operation>

      </wsdl:binding>

      <wsdl:service name="SCCMessageService">
            <wsdl:port binding="impl:SCCMessageSoapBinding"
            name="SCCMessage">
                  <wsdlsoap:address
                  location="http://[redacted]:8081/ARIS/services/SOAP/SCCMessage"/>
            </wsdl:port>
      </wsdl:service>

</wsdl:definitions>
```

commercial info

12.0 COMMERCIAL		High (H) or Medium (M) Priority	Response Category Yes - Accepted No - Not Accepted	Answer/Comments/Explanation
12.1 General Commercial Statements	Where appropriate please indicate your acceptance of the following, and/or provide comments:			
12.1.1	The Contract will be for an initial term of 5 years with the option to extend for a further 2 years.		Yes	
12.1.2	Contract Terms & Conditions - The contract for this requirement will be in accordance with the Crown Commercial Services Framework RM1059/6 Terms & Conditions.		Yes	[redacted]
12.1.3	Contract Order Form - In addition to the contract terms & conditions referred to above , the successful supplier will also be required to sign up to any terms & conditions as specified in the Invitation to tender.		Yes	
12.1.4	Contract documents - Both this invitation to tender, along with the successful supplier's tender and all other relevant documentation will be included in the contract.		Yes	
12.1.5	Please propose figures for liquidated damages to cover potential situations including, but not limited to non – achievement, delay or failure for inclusion in the contract.	H	Open Ended Question	[redacted]
12.1.6	Change Control - Throughout the term of any resulting contract you may progress the inclusion of new services. Such inclusion should be subject to the Council's agreement . Any such changes will be in accordance with the Council's change control procedure.		Yes	
12.1.7	The proposed procurement timetable as stated in section 3.0.		Yes	
12.1.8	Short listed suppliers are expected to carry out a presentation of their proposed solution to a panel of Council representatives, during the 2 weeks commencing December 12th 2016. Please make yourself available to carry out a presentation at all times during those 2 weeks. The Council anticipates visiting reference sites during the period December 12th to 23rd 2016.		Yes	[redacted].
12.1.9	Contract Reviews - The contract for this requirement will necessitate formal Contract reviews to an agreed agenda to monitor the progress of the implementation of the contract and to facilitate change , development or improvement as the contract may require.		Yes	[redacted]
12.1.10	You should provide formal assurance that as from the date of your tender, there is a minimum of 7 years left in the lifecycle of your proposed solution and that there will be full support for all software components for a minimum of 7 years.		Yes	
12.1.11	Software versions no longer under development will be supported for a minimum of 5 years.		Yes	
12.1.12	The Council reserves the right to purchase all third party software required for your proposed solution through its existing contract arrangements		Yes	[redacted]
12.1.13	Minimum insurance levels for this tender are £5million Public Liability, £5million Employers Liability, £2million Professional Indemnity		Yes	[redacted]
12.2 Sub-Contractors	Please provide full details of any sub-contractors which you propose to use for any element of this project. Your response should include:			
12.2.1	Details of any element of the required service to be sub-contracted and the supplier to whom the work will be sub-contracted.	H	Open Ended Question	[redacted] Registered office: 23-38 Hythe Bridge Street Oxford OX1 2EP Telephone: 01865 305200 Email: enquiries@oxfordcc.co.uk Company Registration No: 3521204 Date of registration: 3rd March 1998
12.2.2	Confirmation that all sub-contractor's staff who will undertake such work on behalf of the Council are vetted by you as opposed to being vetted by the proposed sub-contractor and state the processes and procedures involved.	H	Open Ended Question	[redacted]
12.2.3	Acceptance that as prime contractor you accept full responsibility for any and all of the sub-contractors actions.	H	Open Ended Question	[redacted]
12.2.4	Confirmation that the Council reserves the right to reject any nominated sub-contractors and any of the nominated sub-contractors staff.		Yes	
12.2.5	Confirmation that the sub-contractors staff are subject to the same Terms and Conditions as the prime contractor.		Yes	
12.3 Delivery, Installation and Commissioning	Please explain how you are prepared to take responsibility for the following;			

12.3.1	Transport, delivery, installation and commissioning of all supplied software at no additional cost to the Council.	H	Open Ended Question	[redacted]
12.3.2	Installation and commissioning of all software, hardware (if applicable) and material to enable the solution to be implemented in accordance with a mutually agreed schedule of work.	H	Open Ended Question	[redacted]
12.3.3	All third party and open source software that you utilise in your proposal, whether purchased via you or independently.	H	Open Ended Question	[redacted]
12.4 Data Protection	Where appropriate please indicate your acceptance of the following, and/or provide comments:			
12.4.1	Process the Personal Data only in accordance with instructions from the Council (which may be specific instructions or instructions of a general nature as set out in this Agreement or as otherwise notified by the Council to the Contractor during the term of this Agreement).		Yes	
12.4.2	Process the Personal Data only to the extent, and in such manner, as is necessary for the provision of the Services or as is required by Law or any Regulatory Body.		Yes	
12.4.3	Implement appropriate technical and organisational measures, including but not limited to ensuring that Personal Data is not stored on any portable equipment or storage device or media unless encrypted, to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected.		Yes	
12.4.4	Take reasonable steps to ensure the reliability of any contractor personnel who have access to the Personal Data.		Yes	
12.4.5	Obtain prior written consent from the Council in order to transfer the Personal Data to any Sub-contractors or Affiliates for the provision of the Services.		Yes	
12.4.6	Ensure that all Contractor Personnel required to access the Personal Data are informed of the confidential nature of the Personal Data and comply with the obligations set out in the Protection of Personal Data clause.		Yes	
12.4.7	Ensure that no Contractor Personnel publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Council.		Yes	
12.4.8	Notify the Council (within five Working Days) if it receives: a) a request from a Data Subject to have access to that person's Personal Data; or b) a complaint or request relating to the Council's obligations under the Data Protection Legislation.		Yes	
12.4.9	Provide the Council with full cooperation and assistance in relation to any complaint or request made, including by a) providing the Council with full details of the complaint or request b) complying with a data access request within the relevant timescales set out in the Data Protection Legislation and in accordance with the Council's instructions c) providing the Council with any Personal Data it holds in relation to a Data Subject (within the timescales required by the Council); and d) providing the Council with any information requested by the Council.		Yes	
12.4.10	Permit the Council or the Council Representative (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit, in accordance with the Audit clause, the Contractor's data Processing activities (and/or those of its agents, subsidiaries and Sub-contractors) and comply with all reasonable requests or directions by the Council to enable the Council to verify and/or procure that the Contractor is in full compliance with its obligations under this Agreement.		Yes	
12.4.11	Provide a written description of the technical and organisational methods employed by the Contractor for processing Personal Data (within the timescales required by the Council).		Yes	
12.4.12	Not process Personal Data outside the United Kingdom without the prior written consent of the Council and, where the Council consents to a transfer, to comply with a) the obligations of a Data Controller under the Eighth Data Protection Principle set out in Schedule 1 of the Data Protection Act 1998 by providing an adequate level of protection to any Personal Data that is transferred; and b) any reasonable instructions notified to it by the Council.		Yes	
12.4.13	The Contractor shall comply at all times with the Data Protection Legislation and shall not perform its obligations under this Agreement in such a way as to cause the Council to breach any of its applicable obligations under the Data Protection Legislation.		Yes	
12.4.14	The Contractor shall ensure that its employees and agents are aware of and comply with this clause and shall indemnify the Council against any loss or damage sustained or incurred as a result of any breach of this clause.		Yes	
12.5 Continuous Improvement	Regarding continuous improvement:-			
12.5.1	The successful supplier will be required to work with the Council to look into ways of continually improving the solution and the quality of the service that the Council provides to both its internal and external customers. Suppliers are invited to suggest ways that they can work with the Council to develop continuous improvement initiatives.	H	Open Ended Question	[redacted] [redacted] [redacted]
12.6 The Council's Safety Procedures	Regarding the Council's Safety Procedures:-			
12.6.1	Suppliers should state they will ensure that all of their on-site staff complies with the safety procedures as issued to them by the Council		Yes	
12.7 Contractor Staff	Regarding Contractor Staff:-			
12.7.1	Having outlined the reason to the Contractor the Council reserves the right to veto or to require the immediate removal of any of your staff or agents whom the Council deems unsuitable		Yes	
12.8 Freedom of Information	Where appropriate please indicate your acceptance of the following, and/or provide comments:			
12.8.1	The Contractor acknowledges that the Council is subject to the requirements of the FOIA and the Environmental Information Regulations and shall assist and cooperate with the Council to enable the Council to comply with its Information disclosure obligations.		Yes	
12.8.2	The Contractor shall notify the Council of any Commercially Sensitive Information provided to the Council together with details of the reasons for its sensitivity and the Contractor acknowledges that any lists or schedules of Commercially Sensitive Information so provided are of indicative value only and that the Council may be obliged to disclose such information.		Yes	

12.8.3	The Contractor shall and shall procure that its Sub-contractors shall: - Transfer to the Council all Requests for Information that it receives as soon as practicable and in any event within two Working Days of receiving a Request for Information - Provide the Council, at the Contractor's expense, with a copy of all Information in its possession, or power in the form that the Council requires within five Working Days (or such other period as the Council may specify) of the Council's request - Provide, at the Contractor's expense, all necessary assistance as reasonably requested by the Council to enable the Council to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations		Yes	
12.8.4	The Council shall be responsible for determining in its absolute discretion and notwithstanding any other provision in this Agreement or any other agreement whether the Commercially Sensitive Information and/or any other Information is exempt from disclosure in accordance with the provisions of the FOIA or the Environmental Information Regulations and in considering any response to a Request for Information the Council may consult with the Contractor prior to making any decision or considering any exemption.		Yes	
12.8.5	In no event shall the Contractor respond directly to a Request for Information unless expressly authorised to do so by the Council		Yes	
12.8.6	The Contractor acknowledges that (notwithstanding the provisions of this Freedom of Information clause) the Council may, acting in accordance with the Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000 ("the Code"), be obliged under the FOIA, or the Environmental Information Regulations to disclose information concerning the Contractor or the Services: - in certain circumstances without consulting the Contractor; or - following consultation with the Contractor and having taken their views into account; - provided always that where sub-clause above applies the Council shall, in accordance with any recommendations of the Code, take reasonable steps, where appropriate, to give the Contractor advanced notice, or failing that, to draw the disclosure to the Contractor's attention after any such disclosure		Yes	
12.8.7	The Contractor shall ensure that all Information required to be produced or maintained under the terms of this Agreement, or by Law or professional practice or in relation to the Agreement is retained for disclosure for at least the duration of the Agreement plus one year together with such other time period as required by the Agreement, law or practice and shall permit the Council to inspect such records as requested from time to time.		Yes	
12.8.8	The Council shall in no event be liable for any loss, damage, harm, or detriment, howsoever caused, arising from or in connection with the reasonable disclosure under FOIA, or any other Law, of any information (including Exempt Information) whether relating to this Agreement or otherwise relating to any other party.		Yes	
12.8.9	Where the Contractor is a Public Body the parties acknowledges that such obligations and duties of the Council as set out above are reciprocal to the Contractor. The Council and the Contractor acknowledge and agree that: - as Public Bodies they are subject to legal duties under the FOIA and EIR which may require either party to disclose on request information relating to this Agreement or otherwise relating to the other party - they are required by law to consider each and every Request for Information made under FOIA - that all decisions made by the other pursuant to a request under the FOIA are solely a matter for the Receiving Party and at the discretion of the Receiving Party - Notwithstanding anything in this Agreement to the contrary (including but without limitation any obligations or confidentiality), the Receiving Party shall be entitled to disclose information in whatever form pursuant to a request made under FOIA, save that in relation to any information that is Exempt Information the Receiving Party shall consult the other party before making any such decision and shall not: (a) confirm or deny that information is held by the other party, or (b) disclose information required to the extent that in the Receiving Party's opinion the information is eligible in the circumstances for an exemption and therefore the Receiving Party may lawfully refrain from doing either of the things described in part (a) and (b) of this clause each party shall bear its own costs of a) assessing the application of any exemption under FOIA and/or b) responding to any FOIA notice and/or c) lodging any appeal against a decision of the Information Commissioner in relation to disclosure - The Receiving Party shall in no circumstances be liable for any loss, damage, harm, or detriment, howsoever caused, arising from or in connection with the reasonable disclosure under FOIA of any Exempt Information or other information whether relating to this Agreement or otherwise relating to the other party. - The other party shall assist the Receiving Party with the request as reasonably necessary to enable the Receiving Party to comply with its obligations under FOIA		Yes	
12.9 UK Procurement Law and Quality Plans	Where appropriate please indicate your acceptance of the following, and/or provide comments:			
12.9.1	UK Procurement Law and all associated regulations will apply to this procurement.		Yes	
12.9.2	Any elements of supplier Quality Plans that are deemed to be essential to the delivery of the Services will be incorporated within the contract for this requirement.		Yes	
12.11 Payment Terms	Where appropriate please indicate your acceptance of the following, and/or provide comments:			
12.11.1	Payment of all supplier invoices against the contract will be payable within 28 days following receipt of a properly rendered invoice.		Yes	
12.11.2	The Council's proposed payment plan for acceptance of this system as stated in Appendix 2		Yes	
12.11.3	Consultancy Services against the contract will be called off on an 'as and when' required basis and will be billed monthly in arrears.		Yes	
12.11.4	Maintenance Services will be charged from the date of go live of the system and will be payable quarterly in advance during the life of the contract		Yes	
12.12 Further Details	Please provide full details of the following:			
12.12.1	Please provide details of any similar service you have provided to other customers. As part of this requirement suppliers should provide details of 2 reference sites for the Council contact/visit.	H	Open Ended Question	[redacted]

12.12.2	If your offered solution is discontinued and a new system is introduced, what is the policy for customers migrating to the new system? Will the existing licences be transferred free of charge?	H	Open Ended Question	[redacted]
12.12.3	PLEASE DETAIL THE SOFTWARE LICENSING ARRANGEMENTS FOR:- The suggested operating system –The proposed software solution- PLEASE DETAIL; The type and number of software licences offered within your tender proposal- Perpetual licence or if not the term of the licence- Detail any licence restrictions and provide all other licensing details associated with the scope and use of the proposed solution – whether the licences are transferable and if so clearly identify what restrictions there are on the licence use ,if any .	H	Open Ended Question	[redacted]
12.12.4	Please state whether your proposed solution contains any embedded software and if so provide all relevant details.	H	Open Ended Question	[redacted]
12.13 Additional Commercial Comments	Please add any relevant comments not covered above	Value Added Question		[redacted]

Shropshire Council

personal & commercial info

Liquidlogic Ltd
Brookfield House
Selby Road
Leeds
LS25 1NB

Emailed to: [redacted]

Shropshire Council
Shirehall
Abbey Foregate
Shrewsbury
Shropshire SY2 6ND

28 February 2017

Dear Bidder

RMCI 019 - INTEGRATED ADULTS' AND CHILDREN'S SOCIAL CARE CASE MANAGEMENT AND FINANCE SYSTEM
FURTHER COMPETITION THROUGH CROWN COMMERCIAL SERVICES (CCS) FRAMEWORK – RM 1059 – LOT 6 SOCIAL CARE

SHROPSHIRE COUNCIL

SUBJECT TO CONTRACT

This is an Award Decision Notice. We are pleased to inform you that, following the evaluation process, Shropshire Council proposes to accept your offer in relation to the above Contract.

However, this letter is not, at this stage, a communication of Shropshire Council's formal acceptance and a mandatory "standstill" period is now in force; this period will end at midnight on 10 March 2017.

Subject to Shropshire Council receiving no notice during the standstill period of any intention to legally challenge the award process, the Council aims to conclude the award after the expiry of the standstill period.

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted].

We can confirm that your tender received the following scores and ranking:-

commercial & personal info

Criteria	**Your Weighted Score**	**Winning Tenderer's Total Weighted Marks**	**Your Rank** (out of all 3 tenders received)
Quality	[redacted]	[redacted]	[redacted]
Price	[redacted]	[redacted]	[redacted]
Overall	[redacted]	[redacted]	[redacted]

For your further information, we would confirm that your quality submission was scored against the published scoring scheme and the stated award criteria and received the marks as set out on the enclosed spreadsheet. We have also included some commentary in the spreadsheet where marks have been moderated. A Tenderer feedback report is also enclosed and this sets out the process and individual tenderer performances throughout the evaluation stage.

We will be in touch with you again at the end of the standstill period.

Yours faithfully

[redacted]

Director of Adult Services
Shropshire Council

[redacted]
01743 258911

Final Points Awarded in Respect of Procurement Exercise
Moderated Functional (Sections 1.0 to 6.0) - Average Percentage Score (A)
Moderated Non-Functional (Sections 7.0 to 12.0) - Average Percentage Score (B)
Functional Group Score = *A x 500*
Non-Functional Group Score = *B x 350*
Total Moderated Value Added Points
Functional - Assigned Score (where the highest scoring supplier receives 500 points and lower scoring suppliers receive a proportionate amount of points)
Non-Functional - Assigned Score (where the highest scoring supplier receives 350 points and lower scoring suppliers receive a proportionate amount of points)
Price Assigned Score (where the supplier with the lowest ‘whole life cost’ receives 200 points and suppliers with higher ‘whole life costs’ receive a proportionate amount of points)
Total Phase 1 Score

Phase 2 Demo Days Moderated Score
Phase 2 Site Visits Moderated Score
Total Moderated Phase 2 Score

Total Score

[redacted]