



1 November 2017

**Tel:** (01743) 252051

**Fax:** (01743) 255901

Please ask for: [REDACTED]

Email: [procurement@shropshire.gov.uk](mailto:procurement@shropshire.gov.uk)

RONI 003

Dear Sirs

**RONI 003 – WIFI ROLLOUT  
TENDERED UNDER RM1045 LOT 2  
SHROPSHIRE COUNCIL**

You have been invited to tender for the above requirement. With this letter please find copies of the following documents:

1. Instructions for Tendering
2. Short Form Further Competition (SFFC) Order Form
3. Appendix A – Site list and details
4. Appendix B – Floor plan request and agreement
5. Shropshire Council Information Security Policy

Tenders should be made on the enclosed Tender Response Document. 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 pay particular attention to the points below concerning the returning of tenders.

**Returning of Tenders**

- The deadline for returning tenders is **noon on 31 July 2017** 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.**

personal info

Tenders **cannot** be accepted if:

- Tenders are received by post, facsimilie or email
- Tenders 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.

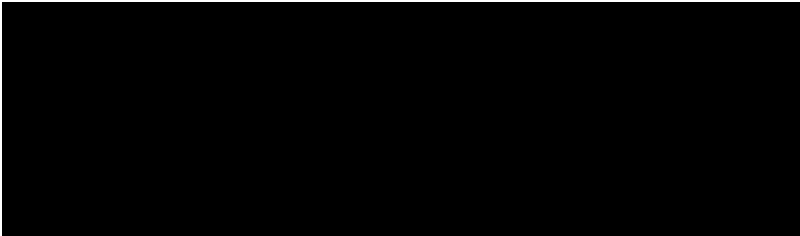
Therefore if you provide any information to Shropshire Council in the expectation that it will be held in confidence, you must make it clear in your documentation as to the information to which you consider a duty of confidentiality applies. The use of blanket protective markings such as "commercial 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



Commissioning Development & Procurement Manager  
Commissioning Development & Procurement  
[procurement@shropshire.gov.uk](mailto:procurement@shropshire.gov.uk)  
Tel: 01743 252993  
Enc



# **INSTRUCTIONS FOR TENDERING**

**RONI 003 – Wifi Rollout  
Tendered under CCS framework  
RM1045 Lot 2**

## Shropshire Council Instructions for tendering

### **Contract Description:**

Shropshire Council requires a corporate Wi-Fi solution which can be installed in its main office (Shirehall). This solution must be capable of being extended to cover other sites the Council may choose to include. Phase 1 of this project will be the setup of the infrastructure and deployment over Shirehall, phase 2 will be extending this to the other sites the Council chooses to include.

## Index

### Contents

1.0 Invitation to Tender .....	2
2.0 Terms and Conditions .....	3
3.0 Preparation of Tenders .....	3
4.0 Tender Submission .....	5
5.0 Variant Bids .....	5
6.0 Tender Evaluation .....	6
7.0 Clarifications .....	6
8.0 Continuation of the Procurement Process .....	7
9.0 Confidentiality .....	7
10.0 Freedom of Information .....	8
11.0 Disqualification .....	9
12.0 E-Procurement .....	10
13.0 Award of Contract .....	10
14.0 Value of Contract .....	11
15.0 Acceptance .....	11
16.0 Payment Terms .....	11
17.0 Liability of Council .....	11
18.0 Committee .....	12
19.0 Declaration .....	12

## 1.0 Invitation to Tender

- 1.1** You are invited to tender for the provision of the rollout of wifi as detailed in the Tender Response Document. The contract will be for an initial period of 3 years commencing on the 1 October 2017 with the option to extend up to the 30 September 2022.
- 1.2** Tenders are to be submitted in accordance with the General Terms and Conditions of CCS Framework RM1045 and the instructions outlined within this document.
- 1.3** 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.
- 1.4** 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.
- 1.5** 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.
- 1.6** 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. 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 any pre-tender questionnaire submitted as part of the formal tender evaluation is hereby reserved by the Council.
- 1.7** 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.
- 1.8** 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

## 2.0 Terms and Conditions

- 2.1** Every Tender received by the Council shall be deemed to have been made subject to the General Terms and Conditions and these Instructions for Tendering unless the Council shall previously have expressly agreed in writing to the contrary.
- 2.2** The Tenderer is advised that in the event of their Tender being accepted by the Council, they will be required to undertake the required services.

## 3.0 Preparation of Tenders

### **3.1 Completing the Tender Response Document**

- 3.1.1** Tenders should be submitted using the 'Tender Response Document' following the instructions given at 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.
- 3.1.2** 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.
- 3.1.3** The Invitation to Tender Documents are and shall remain the property and copyright of the Council

### **3.2 Tender Preparation and Costs**

- 3.2.1** 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.
- 3.2.2** 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.
- 3.2.3** 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.

- 3.2.4** The Council will not be liable for any costs incurred by Tenderers in the preparation or presentation of their tenders.
- 3.2.5** Tenderers are required to complete all pricing schedules in the Invitation to tender documents. 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.
- 3.2.6** 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.
- 3.2.7** 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.
- 3.2.8** 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.
- 3.2.9** 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.

### **3.3 Parent Company Guarantee**

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.

### **3.4 Warranty**

The Tenderer warrants that all the information given in their Tender and if applicable their Request to Participate Questionnaire 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

## 4.0 Tender Submission

- 4.1** 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, 31<sup>st</sup> July 2017**.
- 4.2** No unauthorised alteration or addition should be made to the 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.
- 4.3** 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.
- 4.4** Tenderers should note that their Tender must remain open and valid and capable of acceptance for a period of at least 90 days.
- 4.5** 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.
- 4.6** Where Tender submissions are incomplete the Council reserves the right not to accept them.

## 5.0 Variant Bids

- 5.1** The Council is interested in alternative solutions which would provide and develop opportunities for savings in service costs, service improvement or other financial benefits. In particular, the Council wishes to encourage solutions which also deliver benefits and added value to the local economy, residents and the business community.
- 5.2** Tenderers may submit, at their discretion, a Tender offering a different approach to the project as a "Variant Bid". However, to permit comparability, at least one bid must be submitted strictly in accordance with the Invitation to Tender Documents (the "Compliant Tender"). Any Tender variant proposed must clearly state how it varies from the requirements of the Compliant Tender Documents, and be explicit in demonstrating the benefits that will accrue to the Council from adopting this approach. Tenderers will be required to identify which submission, in their view, demonstrates best value to the Council.
- 5.3** Variant Bids must contain sufficient financial and operational detail to allow any Variant Bid to be compared with the standard Tender, permitting its considerations in written form.



## 6.0 Tender Evaluation

- 6.1** The Tenderers may be called for interview to seek clarification of their tender or additional or supplemental information in relation to their tender. The presentations will not carry any weighting to the final score achieved by Tenderers, but 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 will be reviewed and scores previously awarded will be amended if necessary.
- 6.2** 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.

## 7.0 Clarifications

- 7.1** Tenderers are responsible for clarifying any aspects of the tendering process and/or the Invitation to Tender documents in the manner described below.
- 7.2** If you are unsure of any section and require further clarification, please contact via our Delta Tenderbox.
- 7.3** Where appropriate, the Authorised Officer named above may direct the Tenderer to other officers to deal with the matter.
- 7.4** All queries should be raised as soon as possible (in writing), in any event not later than 21 July 2017.
- 7.5** 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.
- 7.6** 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.

## 8.0 Continuation of the Procurement Process

- 8.1** The Council shall not be committed to any course of action as a result of:
- i) issuing this Invitation to Tender;
  - ii) communicating with a Tenderer, a Tenderer's representative or agent in respect of this procurement exercise;
  - iii) any other communication between the Council (whether directly or through its agents or representatives) and any other party.
- 8.2** 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.
- 8.3** 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. 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.

## 9.0 Confidentiality

- 9.1** 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.
- 9.2** The Contract documents and publications are and shall remain the property of the Council and must be returned upon demand.
- 9.3** Tenderers shall ensure that each and every sub-contractor, consortium member and/or professional advisor to whom it discloses these papers complies with the terms and conditions of this ITT.
- 9.4** The contents of this Invitation to Tender are being made available by the Council on condition that:
- 9.4.1** 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;

- 9.4.2** 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; and
- 9.4.3** Tenderers shall not undertake any publicity activity within any section of the media.
- 9.5** Tenderers may disclose, distribute or pass this Invitation to tender to their professional advisors, sub-contractors or to another person provided that:
- 9.5.1** 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 were the Tenderer; or
- 9.5.2** the Tenderer obtains the prior written consent of the Council in relation to such disclosure, distribution or passing of the Invitation to Tender; or
- 9.5.3** 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
- 9.5.4** the Tenderer is legally required to make such a disclosure.
- 9.6** 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.

**9.7 Transparency of Expenditure**

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.

## 10.0 Freedom of Information

- 10.1** 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.
- 10.2** 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.

- 10.3** 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 should be given.
- 10.4** 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.
- 10.5** 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>

## 11.0 Disqualification

- 11.1** The Council reserves the right to reject or disqualify a Tenderer’s Tender submission where:
- 11.1.1** The tenderer fails to comply fully with the requirements of this Invitation to tender or is in breach of clause 15 of the Council’s General Terms and Conditions relating to Bribery and Corruption or is guilty of a serious or intentional or reckless misrepresentation in supplying any information required; or
- 11.1.2** The tenderer is guilty of serious or intentional or reckless misrepresentation in relation to its tender return and/or the procurement process.
- 11.1.3** 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.
- 11.1.4** The Tenderer :
- a) Fixes or adjusts the amount of his Tender by or in accordance with any agreement or arrangements with any other person; or
  - b) 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
  - c) 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

- d) 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.
- 11.2** 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.
- 11.3** 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.

## 12.0 E-Procurement

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.

## 13.0 Award of Contract

### **13.1 Award Criteria**

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

### **13.2 Award Notice**

The Council will publish the name and addresses of the successful Tenderers in the Official Journal of the European Union (OJEU) where appropriate. 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.

### **13.3 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.

## 14.0 Value of Contract

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

## 15.0 Acceptance

- 15.1** 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.
- 15.2** The Tender documentation including, the CCS RM1045 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.
- 15.3** The Tenderer shall be prepared to commence the provision of the supply and services on the start date of the contract arrangement being 1 October 2017.

## 16.0 Payment Terms

**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.

## 17.0 Liability of Council

- 17.1** The Council does not bind himself to accept the lowest or any tender.
- 17.2** 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.

- 17.3** 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.
  
- 17.4** 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.
  
- 17.5** 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 given 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.

## 18.0 Committee

The Contractor agrees that where requested in writing during the term of any Agreement for the supply 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

## 19.0 Declaration

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 .....





**Appendix B – Confidentiality Undertaking Regarding Floor Plan Request**

**RONI 003 – Wi-Fi Rollout**

[Date]                      2017

[NAME]

Your ref: \*

Our ref: RONI 003

Dear Procurement Team

Please accept this as a request to provide the floor plans relating to the above tender.

We hereby acknowledge that this information is confidential. We undertake: -

1. To treat the information in the strictest confidence
2. That the information will be used solely for the purpose of preparing this Bid
3. That it will not be disclosed to any other party for any purpose whatsoever, and we will not make copies thereof

We acknowledge that all documents and other information received from the Council as detailed above shall remain the Council's property, and that we shall exercise reasonable care to keep them safe from access by unauthorised persons. We shall also return them to the Council forthwith on written request.

**DATED THIS DAY OF**

**Signature**

**Duly authorised to sign for and on behalf of the Bidder (print full name and address of Bidder)**

Please return via Delta or email [procurement@shropshire.gov.uk](mailto:procurement@shropshire.gov.uk)

Clarification site	Qty	Added to Tender_site_list.xls	Allocated from site list	Un-allocated from site sheet
Abbots Wood machines	3	Yes	Abbots Wood (AKA Eskdale House)	
Acton Scott machines	2	Yes	Acton Scott	
Albrighton Library machines	2	Yes	Albrighton Library	
Albrighton Surestart machines	3	Not applicable		
Bayston Hill Library machines	2	Yes	Bayston Hill Library	
Bridgnorth connexions machines	3	Not applicable		Bishops Castle Library
Bridgnorth Highways machines	2	Yes Bridgnorth Highways	Highways Division 4	
Bridgnorth Library machines	12	Yes	Bridgnorth Library	
Broseley Library machines	1	Yes	Broseley Library	
Canterbrook machines	59	Yes	Canter Brook	
Castle View (Inc Oswestry Library) machines	81	Yes	Castle View (including Oswestry Library)	Central Division Longden Road Complex
Church Stretton Library machines	4	Yes	Church Stretton Library	
Church Stretton Surestart machines	1	Yes	Church Stretton Surestart	
Cleobury Library machines	1	Yes	Cleobury Mortimer Library	
CMHT Bridgnorth machines	3	Yes	CMHT Bridgnorth	
CMHT Oswestry machines	3	Yes	CMHT Oswestry SS	CMHT North East
Craven Arms Highways machines	11	Yes – Highways Division 6	CMHT Oswestry SS	
Crowmoor Surestart machines	1	Not applicable	Craven Arms Gateway	Corve Street SS
Edinburgh House Machines	22	Yes	Edinburgh House (Only SC Office)	County Training Ludlow
Ellesmere Library machines	3	Not applicable		

FEC	29	Yes	Food Enterprise Centre	Drovers House
Four Rivers Nursing Home machines	6	Yes	Four Rivers Nursing Home	
Gobowen Library machines	1	Yes	Gobowen Library	
Havenbrook Childrens machines	7	Yes	Havenbrook Childrens Home	
Helena Lane machines	7	Yes	Helena Lane	Harlescott Library (The Lantern)
Highley Library Machines	1	Yes	Highley Library	
Holy Trinity Surestart machines	1	Not applicable		
Idsall Sports Centre machines	2	Yes	Idsall Sports Centre	
Jupiter House machines	18	Yes	Jupiter House	Highways Division 4
Longden Road Machines	56	Yes – Central division	Central Division Longden Road Complex	Highways Division 6
Louise House machines	1	Yes	Louise House	
Ludlow CMHT machines	1	Not applicable		
Ludlow County Training machines	7	Yes	County Training Ludlow	
Ludlow Lib & TIC machines	34	Yes	Ludlow Library	
Ludlow Youth machines	3	Yes	Ludlow Youth Centre	
Market Drayton Lib machines	8	Yes	Market Drayton Library	Ludlow Youth Centre
Meole Brace golf Course machines	2	Yes	Meole Brace Golf course	Market Drayton Connexions
Monkmoor Campus machines	5	Not applicable		
Mt Mckinley machines	170	Yes	Mount McKinley	Market Hall student accomodation
Much Wenlock Library machines	1	Yes	Much Wenlock Library	
Music Hall machines	13	Yes	The Music Hall	

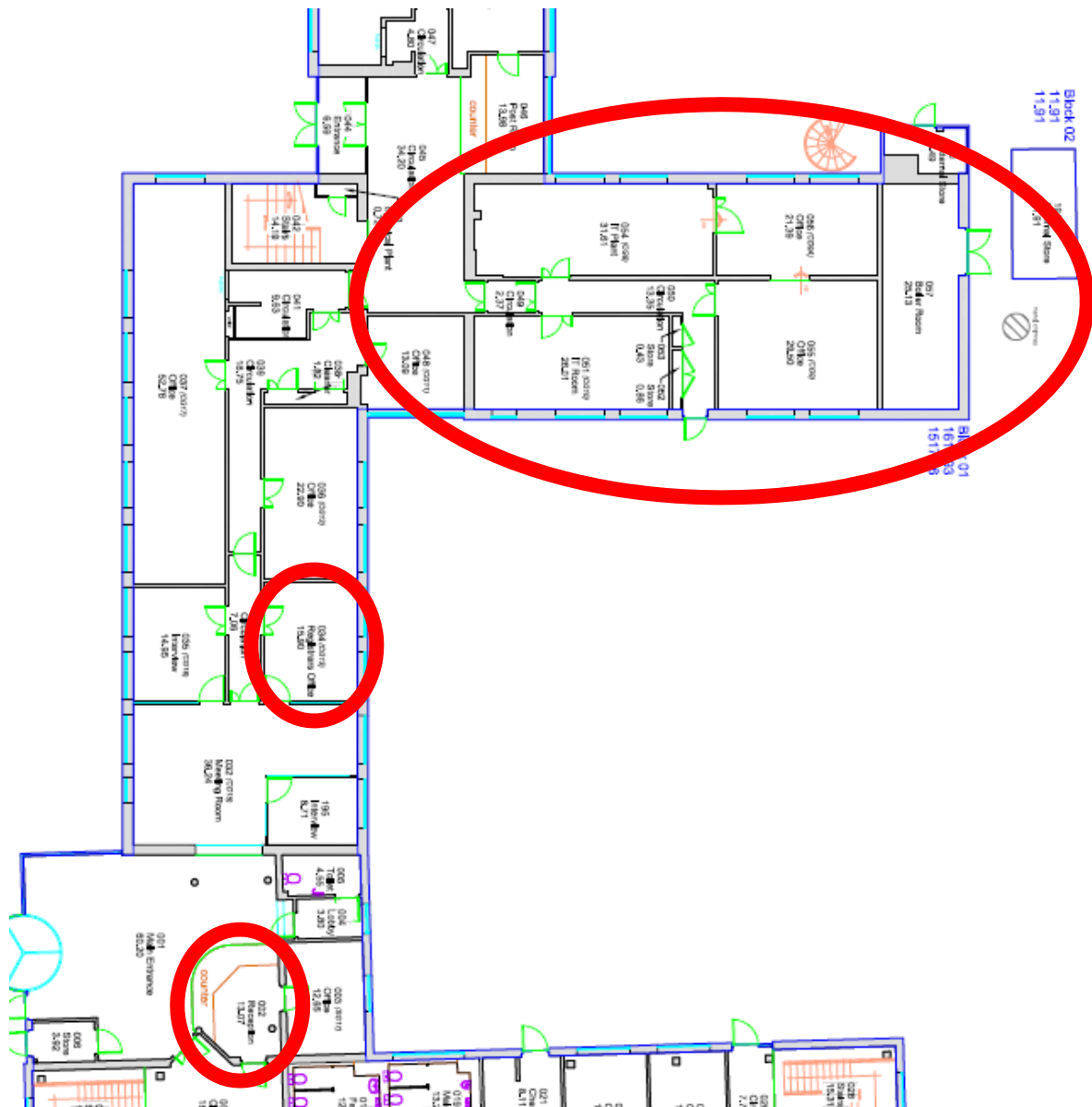
Music&Arts machines	7	Yes	Shropshire Music and Arts Service	
Old Market Hall machines	8	Yes	Old Market Hall	Nuneaton - Centenary Business Centre (Only SC Office)
Oswestry County Training machines	7	Non applicable		
Oswestry Mile End	4	Not applicable		
Oswestry My place machines	16	Yes	Oswestry MyPlace	
Park Hall Depot machines	11	Yes	Park Hall Depot	
Pontesbury Library machines	1	Yes	Pontesbury Library	
Print Unit Atcham	8	Yes	Print Unit Acham	
Ptarmigan machines	116	Yes	Ptarmigan	
Raven house machines	22	Yes	Raven House	
Raven meadows car park machines	1	Not applicable		Royal Shrewsbury Hospital (Only SC Office)
Richmond house machines	14	Yes	Richmond House	
RSH machines	25	Yes Royal Shrewsbury Hospital	Royal Shrewsbury Hospital	
Shifnal Library machines	1	Yes	Shifnal Library	
Shirehall Machines	972	Yes	Shirehall	Shropshire Music and Arts Service
Shrewsbury Library machines	77	Yes	Shrewsbury Library (including archives)	
Shrewsbury Training centre machines	2	Yes	Shrewsbury Training and Development	
Shropshire Hills machines	8	Not applicable		Sunflower House
Shropshire House AONB Drovers	8	Yes	Drovers House	Tannery Replacement building
Spruce House Machines	39	Not applicable		
Stokesay Childrens Centre machines	5	Yes	Stokesay Children's Centre	The Music Hall
Sundorne Surestart machines	1	Not applicable	Sundorne Youth Centre	The Shirehall
Sunflower house machines	14	Yes	Sunflower House	

The Gateway Cravenarms machines	33	Yes	Craven Arms Gateway	
The Gateway Shrewsbury machines	13	Yes	The Gateway (Shrewsbury)	
The Lantern machines	12	Yes	Harlescott Library (The Lantern)	
Theatre Seven machines	23	Yes	Theatre 7	
Weeping cross depot Machines	1	Not applicable		
Wem Childrens Centre machines	1	Yes	Wem Childrens Centre	
Wem Library machines	2	Yes	Wem Library	
Whitchurch Library machines	3	Yes	Whitchurch Library	
Whitchurch Surestart machines	1	Not applicable	Whitchurch Youth Centre	

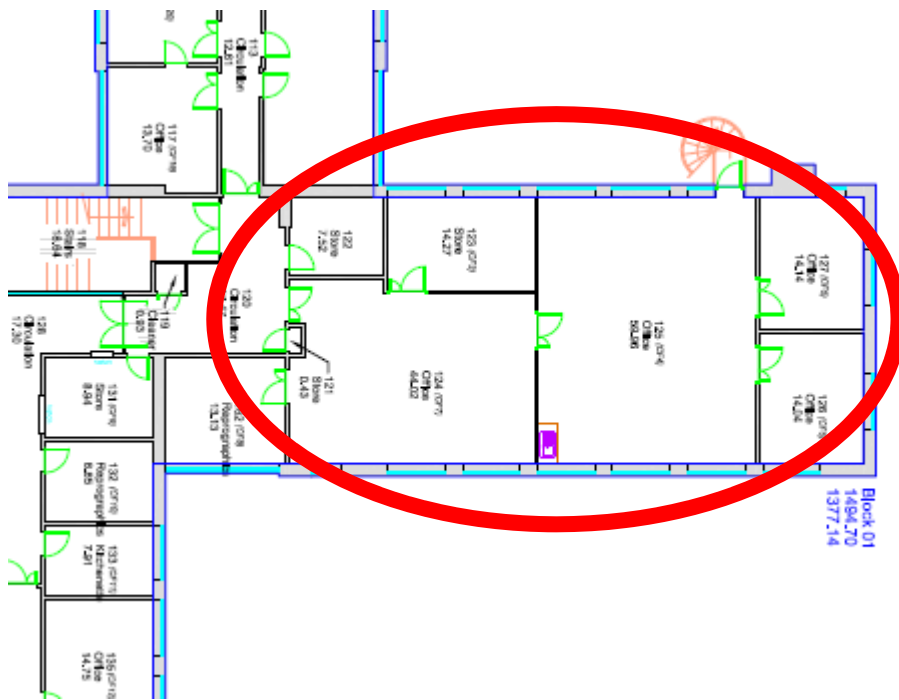
# Edinburgh House

SC staff locations – please refer to the areas circled in Red

## Ground Floor



## First Floor



The area requiring cover on the first floor is directly above the main area on the Ground floor

# **Corporate Information Security Policy**



# Contents

## SECTIONS

1. INTRODUCTION
2. SCOPE
3. POLICY OBJECTIVES
4. SYSTEM ACCESS CONTROL
5. COMMUNICATIONS & OPERATIONS MANAGEMENT
6. SYSTEMS DEVELOPMENT & MAINTENANCE
7. PERSONNEL SECURITY
8. PHYSICAL & ENVIRONMENTAL SECURITY
9. ASSET CLASSIFICATION
10. BUSINESS CONTINUITY MANAGEMENT
11. COMPLIANCE

## APPENDICES

- Appendix A GLOSSARY
- Appendix B INTERNET SECURITY POLICY
- Appendix C INCIDENT CLASSIFICATION
- Appendix D ASSET TYPES
- Appendix E RESPONSIBILITY MATRIX
- Appendix F CRIMINAL RECORDS BUREAU (CRB) INFORMATION POLICY STATEMENT
- Appendix G SECURITY INCIDENT MANAGEMENT PROCEDURES

## 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 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<sup>1</sup> 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

---

<sup>1</sup> 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<sup>2</sup> 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.

---

<sup>2</sup> 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<sup>3</sup> 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.

---

<sup>3</sup> 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

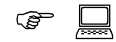


Following the analysis of risks, each Service area should consider and document the impact of each of the threats (specified during the risk analysis) in terms of:

- 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, legislative, 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*



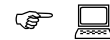
Proprietary software is usually supplied under the terms of a licence agreement that limits their use to specified machines and copying for the purposes of back-up only.

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*

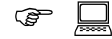


Some records held by the Council such as Tax and VAT details; need to be securely retained to meet with statutory or regulatory enquiries. Responsibility should be established for producing an archive and data retrieval policy in order for the Council to meet the necessary requirements on this subject.

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

<b>Access Control</b>	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.
<b>Audit Trail</b>	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.
<b>Authentication</b>	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).
<b>Authorisation</b>	The granting of rights including the granting of access based on access rights.
<b>Availability</b>	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.
<b>Business Critical Systems</b>	Vital software needed to run the organisation whether custom-written or commercially packaged applications such as accounting, finance, human resources etc.
<b>Business Owner</b>	Individuals, section or department having responsibility for specified information asset(s) and for the maintenance of appropriate security measures
<b>Confidentiality</b>	Protection of sensitive information from unauthorised disclosure
<b>Data</b>	Information. Any series of bit, characters or objects that has meaning. Data is stored and transmitted by computers.

## APPENDIX A

### Glossary

<b>Digital Signature</b>	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
<b>Encryption</b>	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.
<b>Impact</b>	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.
<b>Integrity</b>	Safeguarding the accuracy and completeness of information and software.
<b>Remote Access</b>	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.
<b>Server</b>	A machine whose sole purpose is to supply data so that other machines can use it.
<b>User</b>	Any person who interacts directly with a computer system or uses Information as part of their duties.
<b>User ID</b>	A unique character string that identifies an individual user.

**INTERNET ACCEPTABLE USE POLICY**

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

## 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
<b>Insignificant</b>	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
<b>Minor</b>	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
<b>Significant</b>	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
<b>Major</b>	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
<b>Disastrous</b>	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

## Asset Types

<b>Asset Type</b>	<b>Examples</b>
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 
<b>Sections 1 -3 - Introduction, Scope &amp; Objectives</b>			
	✓	✓	✓
<b>Section 4 - System Access Control</b>			
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	✓	✓	
<b>Section 5 - Communications &amp; Operations Management</b>			
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 
<b>Section 6 - Systems Development &amp; Maintenance</b>			
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	✓		
<b>Section 7 - Personnel security</b>			
7.1.1 Resourcing & 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		✓	✓
<b>Section 8 - Physical &amp; environmental security</b>			
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		✓	✓
<b>Section 9 - Asset Classification</b>			
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 
<b>Section 10 - Business Continuity Management</b>			
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	✓	✓	
<b>Section 11 - Compliance</b>			
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		✓	
<b>Appendices</b>			
<b>Appendix A</b> Glossary	✓	✓	✓
<b>Appendix B</b> Internet Security Policy [superseded by Acceptable Use of Electronic Services Standards].	✓	✓	✓
<b>Appendix C</b> Incident Classification	✓	✓	
<b>Appendix D</b> Asset Types		✓	
<b>Appendix E</b> Responsibility Matrix	✓	✓	✓
<b>Appendix F</b> Disclosure process		✓	
<b>Appendix G</b> 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<sup>4</sup> 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

---

<sup>4</sup> 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.

## 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.



Site	Post code	Address1 - Lead
Abbots Wood (AKA Eskdale House)	SY2 5UA	Abbots Wood (AKA Eskdale H
Acton Scott	SY6 6QQ	Acton Scott
Albrighton Library	WV7 3QH	Albrighton Library
Bayston Hill Library	SY3 0NA	Bayston Hill Library
Bishops Castle Library	SY9 5AQ	Bishops Castle Library, Enterp
Bridgnorth Library	WV16 4AW	Bridgnorth Library
Broseley Library	TF12 5EL	Old School
Cantern Brook	WV16 4SF	Cantern Brook
Shrewsbury Library (including archives)	SY1 2AQ	Shrewsbury Library
Castle View (including Oswestry Library)	SY11 1JR	Castle View
Central Division Longden Road Complex	SY3 9DS	Central Division Longden Roa
Church Stretton Library	SY6 6DQ	Church Stretton Library
Cleobury Mortimer Library	DY14 8PE	Cleobury Mortimer Library, C
CMHT Bridgnorth	WV16 4EU	CMHT Bridgnorth
CMHT Oswestry SS	SY11 2RJ	71 Salop Rd
Corve Street SS	SY8 1DA	Corve Street SS
County Training Ludlow	SY8 1NW	County Training Ludlow
Church Stretton Surestart	SY6 6EX	Church Stretton Surestart
Drovers House	SY7 9BZ	Drovers House
Edinburgh House (Only SC Office)	SY4 5DB	Edinburgh House
Food Enterprise Centre	SY1 3TG	Battlefield enterprise Park
Four Rivers Nursing Home	SY8 1DW	Four Rivers Nursing Home
Gobowen Library	SY11 3NP	Gobowen Library
Havenbrook Childrens Home	SY5 6EP	Havenbrook Childrens Home
Helena Lane	SY8 2NP	Helena Lane
Highley Library	WV16 6JG	Highley Library, Severn Centr
Highways Division 6	SY7 8DU	Highways Division 6
Idsall Sports Centre	TF11 8PD	Idsall Sports Centre

Jupiter House	SY2 6LG	Jupiter House
Louise House	SY3 9JN	Roman Road
Ludlow Library	SY8 2PG	Ludlow Library
Ludlow Youth Centre	SY8 1RT	Ludlow Youth Centre
Market Hall student accomodation	SY1 1QG	Market Hall student accomodation
Market Drayton Connexions	TF9 3AD	Market Drayton Connexions
Market Drayton Library	TF9 1PH	Market Drayton Library
Meole Brace Golf course	SY2 6QQ	Meole Brace Golf course
Mount McKinley	SY2 6LG	Mount McKinley
Much Wenlock Library	TF13 6AE	Much Wenlock Library
The Music Hall	SY1 1LH	The Music Hall
Old Market Hall	SY1 1LH	Old Market Hall
Oswestry MyPlace	SY11 1LW	The Centre
Park Hall Depot	SY11 4AH	Drenewydd
Pontesbury Library	SY5 0TF	Pontesbury Library
Print Unit Acham	SY4 4UG	27 Atcham Business Park
Ptarmigan	SY2 6LG	Ptarmigan
Raven House	TF9 3AH	Raven House
Richmond House	SY1 3QG	Richmond House
Shifnal Library	TF11 8AZ	Shifnal Library
The Shirehall	SY2 6ND	The Shirehall
Shropshire Music and Arts Service	SY3 0NU	Shropshire Music & Arts Serv
Shrewsbury Training and Development	SY2 5BP	Shrewsbury Training and Dev
Stokesay Children's Centre	SY7 9NW	Stokesay Children's Centre, c
Sundorne Youth Centre	SY1 4RG	Sundorne Youth Centre
Sunflower House	SY1 4ES	Sunflower House
Craven Arms Gateway	SY7 9BW	Craven Arms Gateway
The Gateway (Shrewsbury)	SY1 1NB	The Gateway
Harlescott Library (The Lantern)	SY1 4NG	Harlescott Library (The Lante
Theatre 7	SY3 8FT	Theatre 7
Wem Childrens Centre	SY4 5BX	Wem Children's Centre, c/o S
Wem Library	SY4 5AA	Wem Library
Whitchurch Library	SY13 1AX	Whitchurch Library, Town Ha
Whitchurch Youth Centre	SY13 1QL	Whitchurch Youth Centre
CMHT North East	TF9 3DQ	CMHT North East
Highways Division 4	WV15 6AN	Highways Division 4

Nuneaton - Centenary Business Centre (Only SC Office)	CV11 6RY	Centenary Business Centre, H
Royal Shrewsbury Hospital (Only SC Office)	SY3 8XQ	Royal Shrewsbury Hospital
Tannery Replacement building		

Address				
Address2 - Street	Address3 - Town	Address4 - County	Address5- Post code	Floor plan
Eskdale Road	Shrewsbury	Shropshire	SY2 5UA	Yes
Wenlock Edge	Church Stretton	Shropshire	SY6 6QQ	Yes
Station Road	Albrighton	Shropshire	WV7 3QH	Yes
Lythwood Road	Shrewsbury	Shropshire	SY3 0NA	Yes
Station Street	Bishops Castle	Shropshire	SY9 5AQ	Yes
Listley Street	Bridgnorth	Shropshire	WV16 4AW	Yes
Bridgnorth Road	Broseley	Shropshire	TF12 5EL	Yes
Stanley Lane	Bridgnorth	Shropshire	WV16 4SF	Yes
Castle Gates	Shrewsbury	Shropshire	SY1 2AQ	Yes
Arthur Street	Oswestry	Shropshire	SY11 1JR	Yes
107 Longden Road	Shrewsbury	Shropshire	SY3 9DS	Yes
Church Street	Church Stretton	Shropshire	SY6 6DQ	Yes
Love Lane	Cleobury Mortimer	Shropshire	DY14 8PE	Yes
North Gate	Bridgnorth	Shropshire	WV16 4EU	Yes
	Oswestry	Shropshire	SY11 2RJ	Yes - Query
25 Corve Street	Ludlow	Shropshire	SY8 1DA	Yes
Old Street	Ludlow	Shropshire	SY8 1NW	Yes
Shrewsbury Road	Church Stretton	Shropshire	SY6 6EX	Yes
Auction Yard	Craven Arms	Shropshire	SY7 9BZ	Yes
New Street	Wem	Shropshire	SY4 5DB	Yes
24 Vanguard Way	Shrewsbury	Shropshire	SY1 3TG	Yes
Bromfield Rd	Ludlow	Shropshire	SY8 1DW	Yes
St Martins Road	Gobowen, Oswestry	Shropshire	SY11 3NP	Yes
Cound Stank	Shrewsbury	Shropshire	SY5 6EP	Yes
Hamlet Road	Ludlow	Shropshire	SY8 2NP	Yes
Bridgnorth Road	Highley	Shropshire	WV16 6JG	Yes
Longlane Industrial Estate	Craven Arms	Shropshire	SY7 8DU	Yes
Coppice Green Lane	Shifnal	Shropshire	TF11 8PD	Yes

Shrewsbury Business Park	Shrewsbury	Shropshire	SY2 6LG	Yes
Meole Brace	Shrewsbury	Shropshire	SY3 9JN	Yes
7-9 Parkway	Ludlow	Shropshire	SY8 2PG	Yes
Lower Galdeford	Ludlow	Shropshire	SY8 1RT	Yes
Mardol House	Shrewsbury	Shropshire	SY1 1QG	Yes
Drayton Grove	Market Drayton	Shropshire	TF9 3AD	Yes
Cheshire Street	Market Drayton	Shropshire	TF9 1PH	Yes
Oteley Road	Shrewsbury	Shropshire	SY2 6QQ	Yes
Shrewsbury Business Park	Shrewsbury	Shropshire	SY2 6LG	Yes
60 High Street	Much Wenlock	Shropshire	TF13 6AE	Yes
Market Street	Shrewsbury	Shropshire	SY1 1LH	Yes
The Square	Shrewsbury	Shropshire	SY1 1LH	Yes
Oak Street	Shropshire	Shropshire	SY11 1LW	Yes
Park Hall	Oswestry	Shropshire	SY11 4AH	Yes
Bogey Lane	Pontesbury	Shropshire	SY5 0TF	Yes
	Shrewsbury	Shropshire	SY4 4UG	Yes
Shrewsbury Business Park	Shrewsbury	Shropshire	SY2 6LG	Yes
129 Cheshire Street	Market Drayton	Shropshire	TF9 3AH	Yes
Rutland	Shrewsbury	Shropshire	SY1 3QG	Yes
Broadway	Shifnal	Shropshire	TF11 8AZ	Yes
Abbey Foregate	Shrewsbury	Shropshire	SY2 6ND	Yes
Bayston Hill	Shrewsbury	Shropshire	SY3 0NU	Yes
Racecourse Crescent	Shrewsbury	Shropshire	SY2 5BP	yes
Market Street	Craven Arms	Shropshire	SY7 9NW	Yes
Sundorne Road	Shrewsbury	Shropshire	SY1 4RG	Yes
Kendal Road	Shrewsbury	Shropshire	SY1 4ES	Yes
Auction Yard	Craven Arms	Shropshire	SY7 9BW	Yes
Chester Street	Shrewsbury	Shropshire	SY1 1NB	Yes
Meadow Farm Drive	Shrewsbury	Shropshire	SY1 4NG	Yes
Frankwell Quay	Shrewsbury	Shropshire	SY3 8FT	Yes
Shrubbery Gardens	Wem	Shropshire	SY4 5BX	Yes
High Street	Wem	Shropshire	SY4 5AA	Yes
High Street	Whitchurch	Shropshire	SY13 1AX	Yes
Bridgewater Street	Whitchurch	Shropshire	SY13 1QL	Yes
Shropshire Street	Market Drayton	Shropshire	TF9 3DQ	No Plan
Stourbridge Rd	Bridgnorth	Shropshire	WV15 6AN	No Plan

Attleborough Fields Industrial Estate	Nuneaton	Warwickshire	CV11 6RY	No Plan
Mytton Oak Road	Shrewsbury	Shropshire	SY3 8XQ	No Plan
				No Plan

Site Access Information

Hub room marked on plan	Floor plan file name	Network cabinet location
Yes	Abbots_wood.pdf	G.006 Hub Room
Yes on Acton_Scott_2.pdf	Acton_scott.pdf Acton_scott_2.pdf	Café Cupboard Multiple across site in the Gateway Building, Barn and old School House. Exact locations within buildings need confirming
Yes	Albrighton_library.pdf	300 Plant
Yes	Bayston_hill_library.pdf	003 Work Room
Need confirmation	Bishops_castle_library.pdf	003 Library reception or 005 office
Yes	Bridgnorth_Library.pdf	015 Work Room
Yes	Broseley_Library.pdf	010 Library reception
Yes	Canterbrook.pdf	030 IT Suite
Yes	Castle gates library.pdf Shropshire Archives.pdf	Library basement 038 Ground floor - issue desk 028 Archives 076 020
Yes	Castleview.pdf Oswestry Library.pdf	Ground Floor - 010 - IT Room Ground Floor - 178 - Server Ground Floor - 210 - Store Ground Floor - 178 Server Basement / Lower Ground Floor 205 IT Room Ground Floor 053 Electrical Plant Ground Floor 045 Server First Floor 074 Reprographics Second Floor 092 - office Second Floor 088 - store Second Floor 112 - IT Plant Second Floor 152 - Medical Room
Yes	Central_div.pdf	Demountable meeting room 127 Block 01 Room 22 IT Room Block 06 Room 81 Server
Yes	Church_Stretton_Library.pdf	004 Library / 006 Library Reception 013 Office
Yes	Cleobury_Mortimer_Library.pdf	555 Reprographics
	CMHT_Bridgnorth.pdf	Unknown
	CMHT_Oswestry.pdf CMHT_Oswestry_2.pdf	
Yes	Corve_Street.pdf	First Floor 012 Office
Yes	County_training_ludlow.pdf	019 Server
Yes	CS_Childrens_Centre.pdf	556 Store
Query - whole buiding?	Drovers_House.pdf	Unit 13
No	Edinburgh House.pdf	Block 1 054 IT Plant
Yes	FEC.pdf	011 Server
Yes	Four_Rivers.pdf	1.063
Yes	Gobowen_Library.pdf	003 Library Reception
Yes	Havenbrook.pdf	016 office
Yes	Helena_Lane.pdf	G.035
Yes	Highley_library.pdf Highley_Library_2.pdf	005 Store
Yes	Highways_div_6.pdf	011 Office
No	Idsall_sports_centre.pdf	unknown

Yes	Jupiter House.pdf	005 Office
Yes	Louise_House.pdf	G055
Yes	Ludlow Museum and Resource cen	Basement 085 Electrical Plant Second Floor 064 Server
Yes	Ludlow Youth Centre.pdf	017 Store
Yes	Market Hall_student_accomodation	Unknown at this stage
Yes	Market_Drayton_connexions.pdf	Coffee Bar Store Cupboard
Yes	Market_Drayton_Library.pdf	Block 1 002 Library / Block 2 011 Tourist Information
Yes	Meole_Golf.pdf	Office
Yes	Mt McKinley.pdf	First Floor 043 IT Room
Yes	Much_Wenlock_Library.pdf	001 Library
Yes	Music hall.pdf	066 Plant 086 plant
Yes	Old_market_hall.pdf	020 projection room
Yes	Oswestry.myplace.pdf	010 server
Yes	Park_Hall.pdf	017 server
Yes	Pontesbury_Library.pdf	583
Yes	Print_Unit.pdf	<b>B002</b>
Yes	Ptarmigan.pdf	026 Server First Floor 041 Server
Yes	Raven House.pdf	First floor next to toilets (right)
Yes	Richmond_House.pdf	004 Reprographics/013 Office
Yes	Shifnal_library.pdf	Workroom wall behind issue desk)
Yes	Shirehall plans.pdf	Basement B160 Plant Ground Floor GS15 Ground Floor GS53B East Wing GE13 GS126 Swich Gear Room West Wing GW203 IT Room West Wing GW21C Office First Floor North 1N215 Communications Second Floor 2L01 Server Fourth Floor 4S133 Control Room Annex A53 Book Stack
Yes	Shrop_Music.pdf	OAKMEADOW SCHOOL: Caretakers Cupboard
No	STandD.pdf	training room 28, 29 or 30 needs confirming
Yes	Stokesay_CC.pdf	407 Entrance
Yes	Sundorne_Youth.pdf	Interconnecting Meeting Lobby
Yes	Sunflower_House.pdf	First Floor 039 Server
No	The Gateway (Craven Arms).pdf The Gateway (Craven Arms 2).pdf	Behind reception
Yes	The Gateway (Shrewsbury).pdf	029 Office 307 Practical
Yes	The Lantern.pdf	First Floor 057 Plant
Yes	Theatre_severn.pdf	Ground Floor 007 Telecom Room Ground Floor 075 Telecom Room
Yes	Wem_childrens_Centre.pdf	Office
	Wem_library.pdf	009 Server Room
	Whitchurch_library.pdf	003 work room 067 Reception
	Whitchurch_youth_centre.pdf	Reception
		Main Admin Office
N/A		Office



No		Datacentre: Primary Circuit is Cabinet 30F08 . Secondary Circuit is Cabinet 30F06
No		Cupboard, Cavell Suite
No		

Floor	Included in tender	Number of workstations on site
Ground Floor	Yes	3
First Floor	Yes	2
Ground Floor	Yes	2
	Yes	2
Ground Floor	Yes	5
	Yes	12
Ground Floor	Yes	1
First Floor	Yes	59
Basement	Yes	77
Ground Floor	Yes	81
Ground Floor	Yes	56
	Yes	4
	Yes	1
First Floor	Yes	3
First Floor	Yes	3
First Floor	Yes	not documented
Ground Floor	Yes	7
Ground Floor	Yes	1
Second Floor	Yes	8
Ground Floor	Yes	22
	Yes	29
First Floor	Yes	6
Ground Floor	Yes	1
Ground Floor	Yes	7
Ground Floor	Yes	7
Ground Floor	Yes	1
Ground Floor	Yes	11
	Yes	2

Ground Floor	Yes	18
Ground Floor	Yes	1
Top Floor	Yes	34
Ground Floor	Yes	3
437 main entrance 468 Plant	Yes	No staff machines on site - provision of public access wi-fi
Ground Floor	Yes	not documented
Ground Floor	Yes	8
	Yes	2
First Floor	Yes	170
	Yes	1
First Floor	Yes	13
	Yes	8
Ground Floor	Yes	16
First Floor	Yes	11
Ground Floor	Yes	1
	Yes	8
Ground Floor	Yes	116
First Floor	Yes	22
Ground Floor	Yes	14
Ground Floor	Yes	1
Ground Floor	Yes	972
	Yes	7
Ground Floor	Yes	2
	Yes	5
Ground Floor	Yes	not documented
First Floor	Yes	14
Ground Floor	Yes	33
Ground Floor	Yes	13
First Floor	Yes	12
	Yes	23
Ground Floor	Yes	1
Ground Floor	Yes	2
Ground Floor	Yes	3
Ground Floor	Yes	1
Ground Floor	Yes	not documented
	Yes	2

Ground Floor	Yes	1
	Yes	25
	Yes	Not applicable - no staff public wi-fi only

Notes

Notes

This site is a working farm which is a local tourist attraction - number of guest users is unknown

Library - Wi-Fi part of Arts Council grant installed January 2016

Network cabinet location to be confirmed

Network cabinet location not available

6 x staff machines - demand for public access is unknown

New comms room within area plan not up to date

Network cabinet location to be confirmed

1 staff machine based on site - demand for public access is unknown
predominant users at this site will be students so will require direct internet access only
Wi-Fi part of Arts Council grant installed January 2016
Wi-Fi part of Arts Council grant installed January 2016
Wi-Fi part of Arts Council grant installed January 2016
1100 Staff users Number of guest users unknow - estimated 100
Floor plans only include First and second floor where staff are based, the network cabinet is based on the Ground floor in reception
No plans available please provide indicative costs based on 2 APs
no plans available please provide indicative costs based on 2 APs

No plans available please provide indicative cost based on 1 AP

no plans available please provide indicative costs based on 2 APs

No plans available - new build however we may wish to include this site once plans are available - predominant users at this site will be students so will require direct internet access only



**Network Services Agreement RM1045  
Framework Schedule 4  
(Template Order Form and Template Call Off Terms) Part 1b**

## **Short Form Further Competition (SFFC) Order Form**

This Order Form must be used to run a Short Form Further Competition under the Network Services Agreement

Before commencing a Short Form Further Competition and completing this Order Form, please refer to the guidance (**How to complete a short form further competition order form**) provided which is available from the Crown Commercial Service (CCS) website on the agreement web page: <http://ccs-agreements.cabinetoffice.gov.uk/contracts/rm1045>

### **Order Form completion**

The Order Form consists of the following sections, please complete as follows:

#### **Section A – General information**

The Customer must complete the blue boxes in this section before issue to Suppliers.  
The Supplier must complete the grey sections as part of the Short Form Tender Response.

#### **Section B – Details of the requirement**

The Customer must complete this section before issue to Suppliers.

#### **Section C – Location details/requirements**

The Customer must complete this section before issue to Suppliers.

#### **Customer Statement of Requirements**

Please attach your Statement of Requirements as Annex A of the Order Form.

#### **Section D – Supplier response**

Suppliers must complete this section for submission as part of the Short Form Tender Response.

#### **Section E - Call Off Contract award**

The Supplier must complete the grey boxes in this section.  
The Supplier must complete details in the signature box and **sign** before submitting a Short Form Tender Response.  
The Customer must complete and sign this section to award a Call Off Contract to the successful Supplier.  
The Supplier's response should be attached to the Order Form as Annex B





Crown  
Commercial  
Service

## Section A General information

This Order Form is issued in accordance with the provisions of the Network Services Framework Agreement RM1045.

The Supplier shall supply the Services specified in this Order Form to the Customer on and subject to the terms of this Order Form, the appendices to this Order Form, as completed by the Customer, Annex A and Annex B and the Call Off Terms (together referred to as the "Call Off Contract") for the duration of the Call Off Contract Period.

For a Short Form Further Competition the following appendices may apply to the Call Off Contract:

### Appendix 1 - Testing

Annex 2 Test Certificate  
Annex 3 Satisfaction Certificate

- to be completed by both Parties as required throughout the life of the Call Off Contract, where Testing has been requested in section B of this Order Form.

Reference: Direct Award and Short Form Further Competition Call Off Terms, Schedule 4

### Appendix 2 - Variation Form

- to be used, if required, by both Parties throughout the life of the Call Off Contract.

Reference: Direct Award and Short Form Further Competition Call Off Terms, Schedule 12

The Call Off Terms that will apply to the Call Off Contract are as specified in the Direct Award and Short Form Further Competition Call Off Terms (Framework Schedule 4, part 2).

### Customer details

#### Customer Organisation name

Shropshire Council

#### Customer billing address

Your organisation's billing address, please ensure you include a postcode  
Shirehall, Abbey Foregate, Shrewsbury SY2 6ND

#### Customer Representative

The name of your point of contact for this requirement

#### Customer Representative

Please provide full address details, email address and telephone number

The Shirehall, Abbey Foregate, Shrewsbury, SY2 6ND, procurement@shropshire.gov.uk

### Supplier details

#### Supplier name

The Supplier organisation name, exactly as it appears on the Framework Agreement. A document listing all Supplier names and registered addresses has been provided for Customers on the agreement web page.

[Click here to enter text.](#)



**Supplier address**

The Supplier's registered address

[Click here to enter text.](#)

**Supplier Representative**

The name of the Supplier point of contact for this requirement

[Click here to enter text.](#)

**Supplier reference number**

A unique number provided by the Supplier at the time of the Short Form Tender Response. This number should be reported in the financial MI return.

[Click here to enter text.](#)



## Section B Details of the requirement

The following details form the basis of a request for a Short Form Tender Response which will be used to award a Call Off Contract.

Suppliers must refer to the Customer Statement of Requirements when preparing their Short Form Tender Response.

### Lot covered by this requirement

Lot 2

### Customer project reference

Please provide a project reference, this will be used in Management Information provided by Suppliers to assist CCS with Framework management.

RONI 003

### Customer Statement of Requirements (SoR) reference

Please complete a SoR and attach it to this Order Form, please provide the reference number of your SoR.

See Appendix A

### Closing date for Supplier responses

10/07/2017

### Last price paid

Please provide the expenditure in the last full financial year by your organisation covering the services being replaced by this Call Off Contract (if applicable). Please provide any relevant details to explain the figure.

N/A

### Call Off Commencement Date

The Call Off Commencement Date is the date of dispatch of this Order Form, following signature by the Customer. This date can be found in section E of this Order Form.

### Expected Call Off Commencement Date

Please provide an indication of the planned Call Off Commencement Date. This will assist Suppliers in preparing their bid, but if provided is for guidance only.

01/10/2017

### Call Off Initial Period

Any period in Months, up to the maximum Call Off Initial Period of 60 Months

36 months

### Call Off Extension Period

The maximum Call Off Extension Period is 24 Months

24 months

### Implementation Plan required?

Tick as required. See clause 6 of the Call Off Terms

Yes  No

### Quality Plan required?

Tick as required. See clause 8 of the Call Off Terms

Yes  No



### Please note

Selecting, or ticking 'yes' to any of the following options may have cost implications and limit the ability of some Suppliers to respond to your request for a Short Form Tender Response.  
Please ensure you read the guidance (How complete a short form further competition order form') which is available on our agreement web page. Details of the implications and risks of the following options are outlined in this guidance.

### Testing required?

Tick as required. See clause 9 of the Call Off Terms  
If Testing is required the forms attached at appendix 1 (Call Off Schedule 4) will be used by both Parties through the life of the Call Off Contract.

Yes  No

### Appointment of Key Personnel?

Tick as required. See clause 24 of the Call Off Terms

Yes  No

### Service Maintenance Level (SML) option

Indicate required Service Maintenance Level (SML).  
See clause 10 of the Call Off Terms and Schedule 6 of the Call Off Terms  
Level 2

### Bespoke Service Period

The standard period is one Month.  
Please specify any different requirement here. See paragraph 4 of Call Off Schedule 6, Part A.  
[Click here to enter text.](#)

### Additional clause "Security Measures" required?

See Call Off Schedule 13, clause 2.2.1

Yes  No

### Additional clause "Access to MOD Sites" required?

See Call Off Schedule 13, clause 2.2.2. Please complete appendix 3.

Yes  No

### Scots Law required?

Tick as required.  
See Call Off Schedule 13, clause 2.1.1

Yes  No

### Northern Ireland Law required?

Tick as required.  
See Call Off Schedule 13, clause 2.1.2

Yes  No

### Non-Crown Body?

Please indicate if you are a Crown or non-Crown Body.  
See Call Off Schedule 13, clause 2.1.3

Crown Body  Non-Crown Body

### Non FOIA Public Body?

Please indicate if you are an FOIA Public Body or non-FOIA Public Body. See Call Off Schedule 13, clause 2.1.4

FOIA Public Body  Non FOIA Public Body

### Dispute Resolution – role

Please provide details of the role within your organisation (if different from the contact provided in section A of this form) that would deal with Disputes.

See Call Off Schedule 11, clause 3.1 for details.

[Click here to enter text.](#)

### Dispute Resolution - arbitration

The default location for arbitration under this framework is London. If you wish to identify a more convenient location (for you and the Supplier) you are able to do so.

See Call Off Schedule 11, clause 6.4.6

Birmingham is a more convenient location



## Section C

### Location details/requirements

Shropshire Council requires a corporate Wi-Fi solution which can be installed in its main office (Shirehall). This solution must be capable of being extended to cover other sites the Council may choose to include. Phase 1 of this project will be the setup of the infrastructure and deployment over Shirehall, phase 2 will be extending this to the other sites the Council chooses to include.

Refer to appendix A for the full site list, network cabinet locations have been marked with a red circle. We require a formal quote for the Shirehall (this must be based on a full survey of the building). Costs for the other sites are required, these can be based on desktop surveys the site plans for these buildings will be available upon request, in order to obtain these floor plans please complete the agreement which can be found in Appendix B. This agreement stipulates that any floor plans issued as part of this tender will be destroyed by any potential vendor at the end of the tender process.

The below sites are connected on a MPLS WAN utilising BT 21<sup>st</sup> Century networking there are also a small number of sites which have dedicated point to point links to the Shirehall data centre.

Additional sites may be added throughout the duration of the contract.



## Section D Supplier response

Suppliers - use this section to provide any details that may be relevant to the Short Form Tender Response. Please ensure that, your detailed response is attached.

The Supplier response will become Annex B of this Order Form.

### Commercially Sensitive Information

Commercially Sensitive Information relating to the Supplier, its IPR or its business, or which the Supplier is indicating to the Customer that, if disclosed by the Customer, would cause the Supplier significant commercial disadvantage or material financial loss.

### Key Personnel

Please see Customer details in section B to confirm if required. See clause 24 of the Call Off Terms for details

Key Role	Key Personnel Name	Key Personnel telephone number	Key Personnel email address

### Complaint handling

Please provide details of a single contact who will be responsible for Complaint handling as detailed in clause 53 of the Call Off Terms.

Name of key contact	
Job role	
Telephone number	
Email address	
Postal address	

### Dispute Resolution - Supplier

Please provide details of the role within your organisation that would deal with Disputes (if different from the contact given above). See Call Off Schedule 11, clause 3.1 for details.



### Supplier Equipment

Please detail any equipment that will be necessary to provide the Services requested by the Customer. See clause 29 of the Call Off Terms

### Performance Monitoring & Reporting

Please provide details (3.1.1 to 3.1.5) as required in part B of Call Off Schedule 6, paragraph 1.2.

### Total contract value

Please provide an estimated total contract value (for the Call Off Initial Period) as detailed in your attached response to the Customer's Statement of Requirements.

[Click here to enter text.](#)

Please provide a summary breakdown of the total contract value.



## Section E Call Off Contract award

This Call Off Contract is awarded in accordance with the provisions of the Network Services Framework Agreement RM1045.

The Supplier shall supply the Services specified in this Order Form to the Customer on and subject to the terms of this Order Form, the appendices to this Order Form, as completed by the Customer, Annex A and Annex B and the Call Off Terms (together referred to as the “Call Off Contract”) for the duration of the Call Off Contract Period.

### Call Off Contract Commencement Date

The commencement date of the Call Off Contract will be the date of dispatch of this signed Order Form by the Customer to the successful Supplier in accordance with Framework Schedule 5 (Call Off Procedures) paragraph 8 (Call Off Award Procedure).

### SIGNATURES

#### For and on behalf of the Supplier (at submission of Short Form Tender Response)

Name	
Job role/title	
Signature	
Date	

#### For and on behalf of the Customer (at Call Off Contract award)

Name	
Job role/title	
Signature	
Date of dispatch	

Please note that if an Order Form is sent to a supplier by post, the postal address provided on the agreement web page <http://ccs-agreements.cabinetoffice.gov.uk/contracts/rm1045> should be used.

Please see the documents tab, and refer to Suppliers by lot, this document also provides an email address for each supplier.

#### For Supplier use

##### Unique Call Off Contract identifier

A unique Order reference number provided by the Supplier at the time of Call Off Contract award. This number must be reported in the financial MI return.

[Click here to enter text.](#)





Please attach your Statement of Requirements as Annex A of this Order Form.

Please do not embed the document.

### **Statement of Requirements**

#### **Contract Description & Specification:**

This is a further competition under the Network Services Framework RM1045 Lot 2.

A contract for the survey, supply, installation and delivery of an 802.11ac corporate Wi-Fi solution utilising Wave2 access points with dual NIC to allow for resiliency to the Shirehall, with the remaining sites detailed on the location lists will be considered for rollout based upon the cost of the proposed solution. The period of the contract is between 1 October 2017 to 30 September 2020 in the first instance, but with an option to extend for a further 24 month period if desired.

Please note the Council cannot give any guarantee in relation to the value of business to be awarded under this contract.

The proposed solution will need to take into consideration the government recommendations for wireless buildings, please refer to the following link

<https://www.gov.uk/guidance/sharing-workplace-wireless-networks>

However these are to be viewed as option as dependent on the impact to price and end user experience Shropshire council may choose not to adhere to all of those guidelines.

### **Wi-Fi Technical Requirements**

#### **Pre-requisites**

The site survey, hardware supply, installation (of hardware and necessary cabling) and delivery of the Wi-Fi solution is to be provided by the supplier completing the tender. Where alterations to electrical and network cabling is required this will be carried out in partnership with the Councils property services, all work will required to meet up to Council standards

#### **Provision**

We require 100% Wi-Fi coverage in each of the sites included to allow staff/guests to roam without service interruption. The solution will be required to provide access to multiple VLANS via existing WAN connections in place at each site including but not limited to;

- The Councils corporate staff network
- Public internet access
- Guest internet services



### **Survey**

We require each site to have a complete survey provided by the successful vendor to establish the requirements and for the vendor to advise accordingly on the most appropriate deployment of Wi-Fi access points.

### **Hardware provision/Installation**

The supplier is to provide all necessary equipment, cabling services and installation services for the project where necessary.

### **Configuration**

We require the supplier to assist with the initial setup of networks and to provide sufficient training/knowledge transfer to the onsite technical team. The user experience of staff connecting to the corporate network must be seamless and match the existing login process and experience of staff who log onto our wired LAN ie using AD credentials, staff must not have to follow any additional processes or enter additional authentication criteria. Only Shropshire council managed devices, ie those which exist within our Active directory are to be able to connect to the Corporate Wi-Fi provision, the solution must be able to detect that is a managed device and allow it to connect to the necessary VLAN to access corporate traffic without additional VPN or Direct access credentials.

### **Security**

We require all networks to adhere to the Councils security policies. The corporate (staff) network is currently PSN compliant and any solution provided will need to adhere to the PSN requirements. All device and user access on the Wi-Fi will need to be logged with a view to being reported on. There should be a dashboard for easy real-time monitoring accessible to IT staff.

### **Training and support**

We require the option for ongoing support at various levels as detailed below:

- Fully managed
- Hardware and Infrastructure support
- Configuration support

Training must also be provided on the proposed solution to enable ICT staff to be able to support the platform.

### **Additional features**

The proposed solution must have the capability to use location based services although the council may choose not to activate these during the initial implementation.

The Council require the facility to advertise services on the public and guest Wi-Fi networks - this may be though such features as splash pages and banners although other advertisement offers will be considered. We require the ability to report on usage of all the networks, including device type and usage. We will also require the ability to filter/block access to websites by category on the public and guest networks.



Please attach a copy of the Supplier's response, as Annex B of this Order Form.

Please do not embed the document.

**Instructions for the completion of this document**

1. This document must be completed in its entirety with responses being given to all questions. If you are unsure of any section/question and require further clarification, please contact us via our Delta Tenderbox. You are recommended to keep a copy of all tender documents and supporting documents for your own records.
2. Tenderers must also complete and sign the four certificates in Sections A1 to A4. These 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.
3. All questions require specific responses from you relating to the organisation named in Section B Question 1.1. All information supplied must be accurate and up to date. The Council reserves the right to refuse to consider your application if the Tender Response Document is not fully completed or is found to be inaccurate.
4. Where copies of certificates and other details are requested **a copy must** accompany the electronic copy of your Tender Response Document.

**Contents**

Section	Description	Page
A1	Form of Tender	23
A2	Non-Canvassing Certificate	24
A3	Non-Collusive Tendering Certificate	25
A4	Declaration of Connection with Officers or Elected Members of the Council	26
<b>You must sign all 4 certificates in sections A1 to A4</b>		
B	Supplier Information– For information only	27
C	Tender Schedule	29
D	Access to information or systems by third parties	40



### **Selection Criteria - Pass/Fail Questions**

This information will be provided for proof of compliance and will be judged on a pass or fail basis. Tenderers must comply with these issues to demonstrate their proven competence, financial stability, resources and other arrangements. Questions marked 'For information only' will not be assessed; however they must still be answered in full.

<b>Section / Question No.</b>	<b>Selection Criteria</b>
Section C / 3.4	Adequate engineer scheduling & support
Section D	Signing of access agreement

Section C: If, in the opinion of the Contracting Authority the responses in this section are sufficiently poor as to cast serious doubt on the Applicant's abilities to perform this contract they may be excluded.

### **Award Criteria – Weighted Marked Questions**

Tenders will be evaluated on the answers provided in this Tender Response Document and judged against the criteria shown in the table below. The following award criteria is made up of 'Quality' and 'Price' and shows how each criteria is to be weighted against each other.

<b>Section / Question No.</b>	<b>Selection Criteria</b>
Section B	Supplier Information– For information only

<b>Section / Question No.</b>	<b>Award Criteria</b>	<b>Weighting / Max Marks Available</b>
<b>Price 30% (300 marks)</b>		
Section C / Q 1	Price	30% / 300 max marks
<b>Total for price</b>		<b>30% / 300 max marks</b>
<b>Quality 70% (700 marks)</b>		
Section C / Q 2	Pre-Requisites	10% / 100 max marks
Section C / Q 3	Customer Experience	15% / 150 max marks
Section C / Q 4	Security	15% / 150 max marks
Section C / Q 5	DR/BC	10% / 100 max marks
Section C / Q 6	Support	10% / 100 max marks
Section C / Q 7	Technical	10% / 100 max marks
<b>Total for quality</b>		<b>70% / 700 max marks</b>

### **Quality Questions/ Scoring Scheme**



Questions within the quality sections shown above will be scored using the following scoring scheme. Each answer from the questions identified below will be given a mark between 0 and 10 with the following meanings:

Assessment	Mark	Interpretation
<b>Excellent</b>	<b>10</b>	<i>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 added value, with evidence to support the response.</i>
	<b>9</b>	
<b>Good</b>	<b>8</b>	<i>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 added value, with evidence to support the response.</i>
	<b>7</b>	
<b>Acceptable</b>	<b>6</b>	<i>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.</i>
	<b>5</b>	
<b>Minor Reservations</b>	<b>4</b>	<i>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.</i>
	<b>3</b>	
<b>Serious Reservations</b>	<b>2</b>	<i>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.</i>
	<b>1</b>	
<b>Unacceptable</b>	<b>0</b>	<i>Does not meet the requirement 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.</i>

The use of odd numbers indicates an answer's allocated mark lies between definitions.



**The tender receiving the highest mark for Quality Criteria overall will receive the full 70% /700 marks available for Quality. Other tenders will receive a % mark that reflects the difference in the marks between those tenders and the tender receiving the highest mark for Quality overall.**

### **Price Evaluation and scoring**

Our indicative requirements have been provided to provide a “basket”. Tenders will be assessed on the total price of the basket (which is unit price x quantity).

The most competitively priced tender will receive the maximum mark for price being **30%/300. Less competitive tenders** will receive a % of the maximum mark that represents the difference in cost between that tender and the most competitively priced tender.



**Section A:**  
**1. Form of Tender**

Form of Tender

**Shropshire Council**

Tender for supply of Wi-Fi Rollout Service

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 rollout of a wi-fi service at the prices and terms agreed and subject to the terms of the invitation to tender documentation and the framework terms RM1045, copies of which we have received.

Signed ..... Name.....

Date .....

Designation .....

Company.....

Address

.....

.....

.....

Post Code .....

Tel No .....

E-mail address .....

Web address.....



**Section A:**

**2. 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 .....





**Section A:**  
**3. 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 .....



**Section A:**

**4. 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 .....	



**SECTION B**

**1. 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	<input type="checkbox"/> Yes
	ii) a limited company	<input type="checkbox"/> Yes
	iii) a limited liability partnership	<input type="checkbox"/> Yes
	iv) other partnership	<input type="checkbox"/> Yes
	v) sole trader	<input type="checkbox"/> Yes
	vi) other (please specify)	<input type="checkbox"/> 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)	<input type="checkbox"/> Yes
	ii) Small or Medium Enterprise (SME) <sup>1</sup>	<input type="checkbox"/> Yes
	iii) Sheltered workshop	<input type="checkbox"/> Yes
	iv) Public service mutual	<input type="checkbox"/> Yes

<sup>1</sup> See EU definition of SME: <http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/>



**1.2 Contact details**

Supplier contact details for enquiries about this tender

Name

Postal  
address

Country

Phone

Mobile

E-mail



## SECTION C – TENDER SCHEDULE

1.	<b>Pricing Schedule – 300 marks - 30%</b>	
1.1	<p>We require the successful tender to give a cost per site based on the sites detailed in this document along with any others the council may choose to include at a later date.</p> <p>Indicative pricing based on a desktop survey utilising provided site plans will be accepted with the exception of Shirehall, a full physical site survey will be required for this site.</p> <p>Please detail the price per site below:</p> <p><b>Refer to appendix A</b></p>	<b>200 Marks</b>
1.2	<p>For each site please provide a breakdown of what the costs include, i.e. number and location of APs, additional cabling, ongoing support and maintenance etc.</p>	<b>50 Marks</b>
1.3	<p>Please detail the costs of any licencing requirements for the proposed solution, including whether the licencing will be perpetual or based on subscription:-</p>	<b>50 Marks</b>



<b>2.</b>	<b>Pre-requisites – 100 marks - 10%</b>	
2.1	<p>Can you provide <b>all</b> of the following services as part of your offering:</p> <ul style="list-style-type: none"><li>• Site survey</li><li>• Provision of all hardware required<ul style="list-style-type: none"><li>○ APs</li><li>○ Cables</li><li>○ Etc</li></ul></li><li>• Coordinate the installation of any network cabling identified as part of the rollout</li><li>• Work in conjunction with in house technical team to design/build the environment including testing to ensure the solution meets our requirements</li><li>• Provide handover and training to in-house technical team during the deployment and once the rollout is complete</li><li>• Provide ongoing support at the required levels</li></ul> <p>For each of the points listed above, please detail the processes you would follow:-</p>	<b>100 Marks</b>
<b>3</b>	<b>Customer Experience - 150 marks - 15%</b>	
3.1	<p>As detailed in our requirements we require users to connect to a single SSID which would then filter the device/user to the necessary network, please give full details of what the user would experience of this for each of the proposed networks, corporate, guest and public networks. The answer should include but is not limited to the following:</p> <ul style="list-style-type: none"><li>• Screen shots of the user interface</li><li>• Details of splash screens</li></ul>	<b>100 Marks</b>
3.2	<p>We would like to utilise location services to report on user location/activity and provide location based advertising and services. Please describe what options are included with your offering and potential usage scenarios for a local authority.</p>	<b>50 Marks</b>



<b>4 Security - 150 marks - 15%</b>		
4.1	<p>We require the wireless network to present a single SSID, the destination VLAN should be determined by 'onboarding' rules based on device and user credentials, please explain how you would achieve this.</p> <p>Your answer should include for example how your proposal would determine between a corporate/managed/private device, establish if anti-virus is up to date</p> <p>If this is not optimal via a single SSID, please outline your alternative proposal giving full details of user experience and any additional technical requirements:-</p>	<b>40 Marks</b>
4.2	<p>The solution must not impact on the Councils continued PSN compliance, please detail how your solution meets PSN standards</p>	<b>50 Marks</b>
4.3a	<p>We require the solution to have the capacity to detect and alert on rogue devices and APs, please detail how your solution achieves this</p>	<b>15 Marks</b>
4.3b	<p>The solution must also allow us to disconnect and blacklist/whitelist any devices/users, please describe the process to do this.</p>	<b>15 Marks</b>



4.4a	Please give a full example of the management interface of your solution, including status dashboards and reporting modules your system provides.	<b>15 Marks</b>
4.4b	We currently use PRTG to monitor our network, can the proposed solution provide SNMP/SNMP/API to produce statistics	<b>15 Marks</b>
<b>5</b>	<b>DR/BC - 100 marks - 10%</b>	
5.1	<p>The system is required to provide resiliency in the event of an</p> <ul style="list-style-type: none"><li>• AP failure</li><li>• AP network loss</li><li>• Controller failure</li><li>• Failure of primary data centre</li></ul> <p>Please describe how your solution fits each of the above requirements including details of any additional costs. Please also map out any processes we would need to implement for any of the above scenarios:-</p>	<b>75 Marks</b>





5.2	Please describe what the user experience would be in the event of an AP failure including any error notifications they may receive and what steps if any they would need to take to regain connectivity:-	<b>25 Marks</b>
<b>6</b>	<b>Support/Training - 100 marks - 10%</b>	
6.1	Please detail all of the training material which will be provided as part of the project including details of any training courses that staff may be able to attend and along with associated costs:-	<b>25 Marks</b>
6.2	We require the option to purchase ongoing support.  Please detail the support options available with associated costs:-	<b>25 Marks</b>
6.3	Please detail the incident resolution and escalating processes:-	<b>25 Marks</b>
6.4	In the event of an AP Hardware failure please outline the replacement process, including details on timescales:-	<b>25 Marks</b>
<b>7</b>	<b>Technical - 100 marks - 10%</b>	



7.1	The POE switches used by Shropshire Council are CISCO and have a total power budget of 370W with the ability to provide either 12 ports of 30W or 24 ports of 15.4W. The APs you recommend must adhere to these power requirements, please give details below:-	<b>30 Marks</b>
7.2	It is possible that additional CISCO POE switches may be required as part of this project.  Please provide an example unit cost for a CISCO POE switch which meets the requirements detailed in Q7.1:-	<b>5 Marks</b>
7.3	In the event where it is not economical to install a POE switch due to a low number of access points required, please provide unit costs for power injectors for your AP:-	<b>5 Marks</b>
7.4	There will be areas which will have a high density of connected devices.  Please provide details of the APs you have recommended, including the maximum recommended number of devices each AP will support, along with maximum recommended throughput:-	<b>20 Marks</b>
7.5	Please detail what your recommended support subscription provides us, i.e. ongoing upgrades, software and firmware updates to APs and other hardware updates to the central management console. Please detail full costs for your support subscription:-	<b>20 Marks</b>



7.6	As stated above, the sites are connected utilising an MPLS WAN or point to point link. If we were to use your provision to service a site that had internet provision only, how would this be achieved? Please detail in your answer any additional costs this may incur and any additional infrastructure that may be needed by us:-	<b>20 Marks</b>
-----	---	-----------------



## **Appendix**

Appendix A – Site list and details

Appendix B – Floor plan request and agreement



**Section D - Access to information or systems by third-parties**

**Please note – this is a Pass/Fail requirement**

This agreement should be signed by all third-parties prior to access being granted to systems and/or non-public Council information. By signing this form you are agreeing:

- to comply with the Council's Information Security Policy and procedures and take all necessary organisational and technical steps to ensure the security integrity and confidentiality of all data and other information held by the Council to which you shall have access
- to conform to the provisions of all relevant legislation inclusive of but not limited to the Data Protection Act 1998, Copyright Designs and Patents Act 1988, Computer Misuse Act 1990 and all subsequent relevant legislation
- that you will not without the prior written consent of the Council, divulge data or any other information provided to you by the Council or held by the Council to which you shall have access
- that you will take all reasonable precautions to ensure that viruses or other malicious software are not introduced onto or into the Council's IT facilities or systems
- that you will not without the previous consent of the Council in writing make any change or alteration to I.T. facilities or systems used by the Council
- that you will not access any of the Council's data information systems or facilities unless you are required to do so and in any event not without the Council's prior consent in writing. This includes only accessing information or systems specified by the Council and in accordance with agreed times of access.
- that you will not disclose methods of access to facilities or systems to any person without the Council's prior consent in writing
- that you will only download, print, copy or export the Council's accessed data or other information in accordance with business requirements agreed in writing with the Council
- that you will not store personal or sensitive data on portable media (CDs, memory sticks, laptops, etc.) without the data being encrypted, not just password protected.

I shall fully indemnify Shropshire Council against all damages (excluding consequential damages), costs, charges and expenses arising from or incurred by any failure on my part to comply with the above clauses and shall promptly notify Shropshire Council in writing of any alleged infringement of which I have notice of.

Notwithstanding the above clause the Contractor will have in place, and will maintain, with a reputable insurer, Public Liability Insurance in the sum of £5,000,000 (FIVE MILLION POUNDS) and Product liability Insurance in the sum of £5,000,000 (FIVE MILLION POUNDS) and Professional Indemnity Insurance in the sum of £1,000,000 (ONE MILLION POUNDS) and will provide evidence of this to Shropshire Council on request. The indemnity given shall be limited to those sums stated.

I agree not to make any admissions of liability without Shropshire Council's prior written consent. The provisions of this Clause shall survive the expiration or termination of this or any related Agreement. Please sign below to acknowledge that you have read and understood this document and agree to the conditions therein.

System or information being accessed: .....

Signed by ..... Print Name.....

Authorised signatory on behalf of the Contractor

Date..... Organisation/Contractor' details.....



**CALL OFF SCHEDULE 4: TESTING**

**ANNEX 2: TEST CERTIFICATE**

To: [insert name of Supplier]  
From: Shropshire Council  
[insert Date dd/mm/yyyy]

Dear Sirs,

**TEST CERTIFICATE**

Deliverables:

**As per page 5, we don't believe testing is required for this contract. If testing is identified as a requirement, then this test certificate will be used**

We refer to the agreement ("**Call Off Contract**") relating to the provision of the Services between Shropshire Council ("**Customer**") and [insert Supplier name] ("**Supplier**") dated [insert Call Off Commencement Date dd/mm/yyyy].

The definitions for terms capitalised in this certificate are set out in this Call Off Contract.

[We confirm that all of Deliverables listed above have been tested successfully in accordance with the Testing Strategy Plan relevant to those Deliverables.]

[OR]

[This Test Certificate is issued pursuant to paragraph 13.1 of Call Off Schedule 4 (Testing) of this Call Off Contract on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]\*

Yours faithfully

[insert Name]

[insert Position]

acting on behalf of Shropshire Council



**CALL OFF SCHEDULE 4: TESTING**

**ANNEX 3: SATISFACTION CERTIFICATE**

To: [insert name of Supplier]  
From: Shropshire Council  
[insert Date dd/mm/yyyy]

Dear Sirs,

**SATISFACTION CERTIFICATE**

Milestone:

**[Guidance Note to Customer: Insert description of the relevant Milestones]**

We refer to the agreement ("**Call Off Contract**") relating to the provision of the Services between Shropshire Council ("**Customer**") and [insert Supplier name] ("**Supplier**") dated [insert Call Off Commencement Date dd/mm/yyyy].

The definitions for terms capitalised in this certificate are set out in this Call Off Contract.

[We confirm that all the Deliverables relating to Milestone [number] have been tested successfully in accordance with the Testing Strategy Plan relevant to this Milestone [or that a conditional Test Certificate has been issued in respect of those Deliverables that have not satisfied the relevant Test Success Criteria.]]\*

[OR]

[This Satisfaction Certificate is granted pursuant to paragraph 13.1 of Call Off Schedule 4 (Testing) of this Call Off Contract on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]\*

[You may now issue an invoice in respect of the Milestone Payment associated with this Milestone in accordance with the provisions of Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing)]\*

**[\*Guidance Note: delete as appropriate]**

Yours faithfully

[insert Name]

[insert Position]

acting on behalf of Shropshire Council



**CALL OFF SCHEDULE 12: VARIATION FORM**

No of Order Form being varied:

.....

Variation Form No:

.....

BETWEEN:

**Shropshire Council** ("the Customer")

and

**[insert name of Supplier]** ("the Supplier")

1. This Call Off Contract is varied as follows and shall take effect on the date signed by both Parties:

**[Guidance Note: Insert details of the Variation]**

- 2. Words and expressions in this Variation shall have the meanings given to them in this Call Off Contract.
- 3. This Call Off Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the Customer

Signature

Date

Name (in Capitals)

Address

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature

Date

Name (in Capitals)

Address





personal & commercial info

Pinacl Solutions UK Ltd  
Pinacl House  
Carlton Court  
St Asaph Business Park  
St Asaph  
Denbighshire  
LL17 0JG  
Emailed to: [REDACTED]

Shropshire Council  
Shirehall  
Abbey Foregate  
Shrewsbury  
Shropshire SY2 6ND

11<sup>th</sup> October 2017

Dear Bidder

**RONI 003 – WIFI ROLLOUT  
TENDERED UNDER CCS FRAMEWORK RM1045 LOT 2  
SUBJECT TO CONTRACT**

Further to your recent submission of a Tender for the above Further Competition carried out under the Crown Commercial Service Network Services (RM1045) framework, 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 the Council will obey a voluntary "standstill" period which is now in force; this period will end at 23:59 on 23rd October 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.

This award notification is also subject to you now providing copies of your relevant insurance certificates together with confirmation from your insurance brokers that:-

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

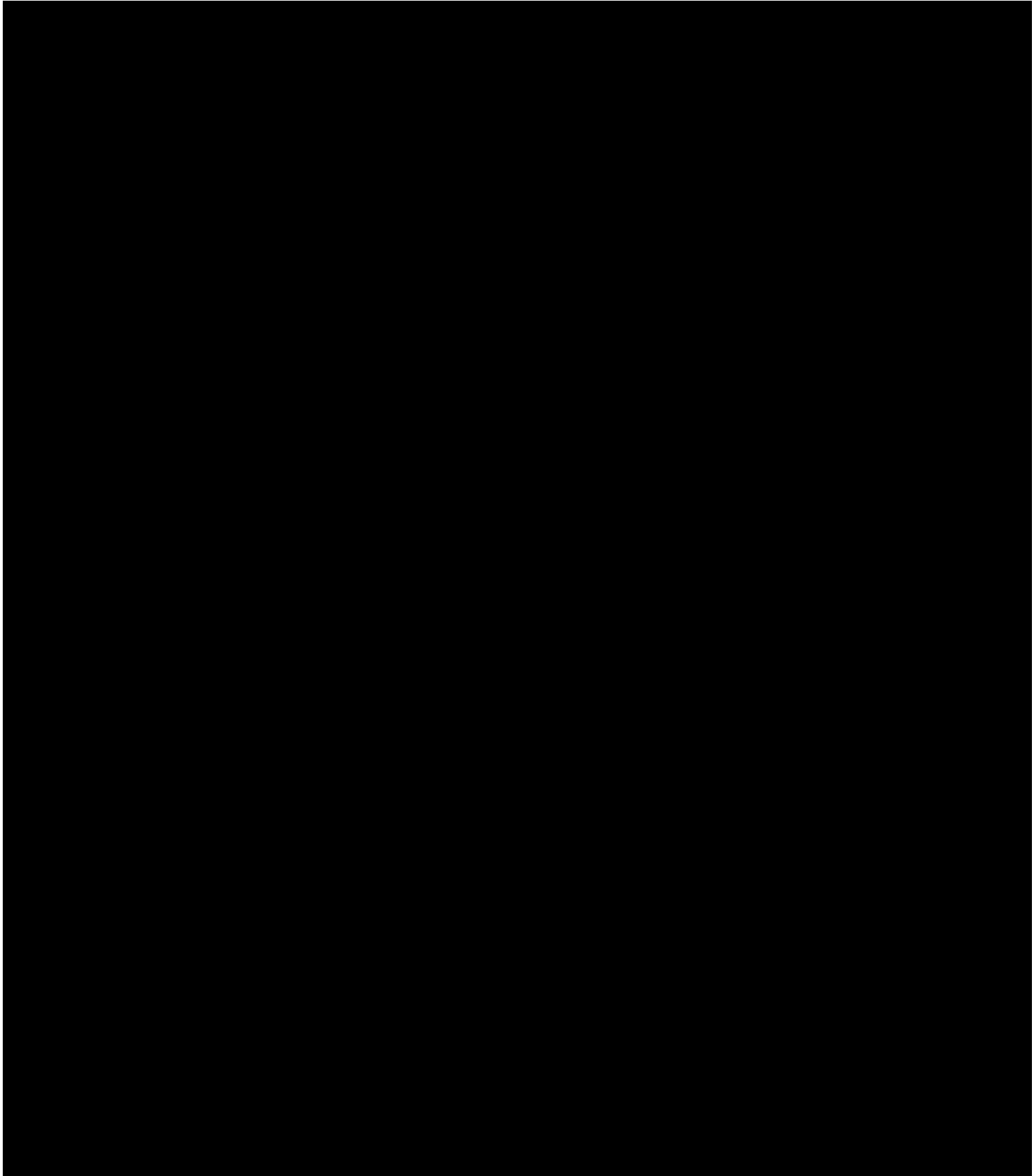
We can confirm that your tender received the following scores and ranking:-

Criteria	Your Weighted Score	Highest Weighted Score	Your Rank (out of all 6 tenders received)
Price Q1.1	■	■	■
Price Q1.2 & 1.3	■	■	■
Quality	■	■	■
Overall	■	■	■

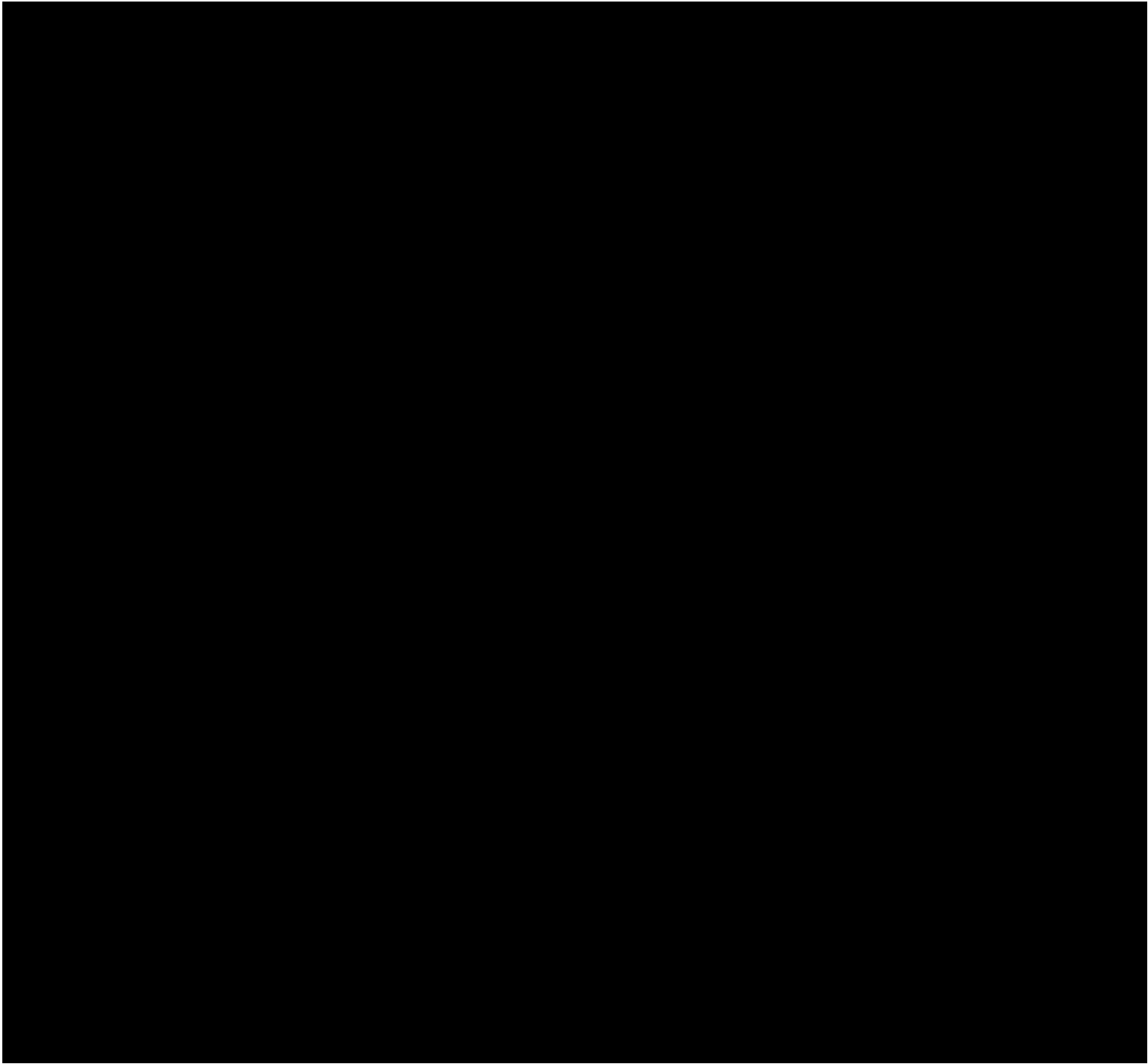


commercial info

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 set out below:



commercial info



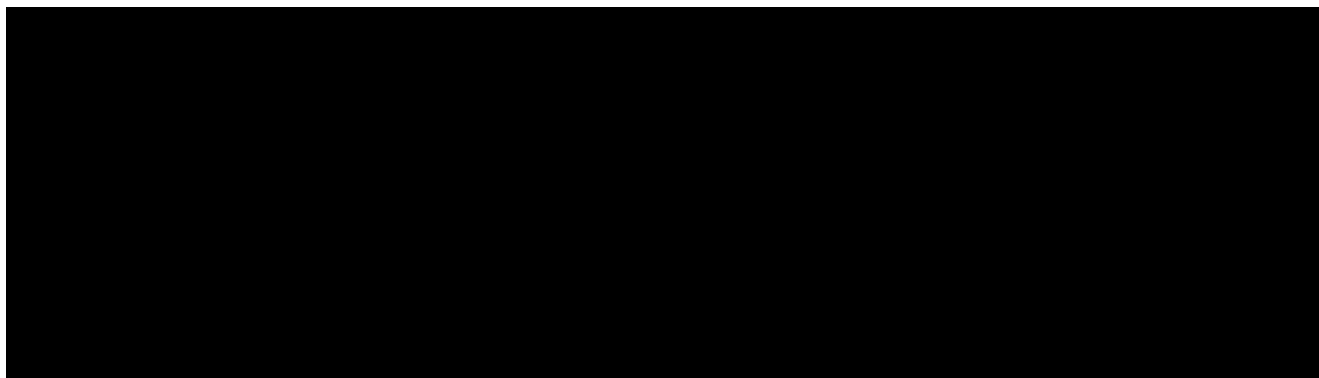
[Redacted signature line]

A copy of the completed Contract will be forwarded to you shortly for your signature and return.

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

Yours faithfully

personal info



Technology and Communications Manager  
Shropshire Council

ICT Service Desk Manager  
Shropshire Council