CITY OF WOLVERHAMPTON

Appendix 2 Specification

INVITATION TO TENDER FOR THE PROVISION OF A MANAGED CLIENT CASELOAD INFORMATION SYSTEM AND TRACKING SERVICE

Contract Number CWC19041

SPECIFICATION

1. Introduction

1.1. This procurement is for the provision of a Connexions Client Caseload Information System (CCIS) and a tracking service that must be operational on 1st October 2019. The supplier will provide full implementation of the system including management and tracking, on-going maintenance, training, data migration and cleansing and report production as specified.

2. Connexions Caseload Information System (CCIS)

2.1. CCIS is essentially a local database that provides Local Authorities with the information they need to support young people to engage in education and training; to identify those who are not participating and to plan services that meet young people's needs. It also enables local authorities to provide management information to the Department of Education (DfE) through the National Client Caseload Information System (NCCIS). Information recorded in NCCIS is used to:

2.1.1. Monitor the extent to which young people are meeting the duty to participate in education or training. This requires pupils who reached the compulsory school leaving age in their summer leaving year and beyond to continue in full time education or training, an apprenticeship, or full-time employment combined with part time study until at least their 18th birthday.

2.1.2. Produce monthly tables which are available on the NCCIS portal for services to compare and benchmark their performance against others.

2.1.3. Produce tables relating to participation, young people not in education, employment or training (NEET) and the September Guarantee which are made available on GOV.UK.

2.1.4. Combine with other administrative data to produce KS4 and KS5 destination measures and the NEET Quarterly Brief.

2.2. The solution needs to be the latest generation software so as to provide scope for further enhancement and development to meet the changing needs of the Council's Connexions Service. The CCIS will be used by the Council's operational staff (approx. 15) who will enter information into the CCIS.

2.3. The system provider will provide a CCIS which is compliant with the specification and data catalogue drawn up by DfE and ensure it meets the data needs of the Council, see link https://www.gov.uk/government/publications/nccis-management-information-requirement. The CCIS and the management of the CCIS must be compliant with the requirements of General Data Protection Regulation requirements.

2.4. The CCIS provider must be able to provide the necessary levels of support for the CCIS installation, maintenance, training, data migration and cleansing, and report development during but not restricted to, the implementation of the proposed CCIS.

2.5. The CCIS should be able to be accessed through the use of an appropriate Internet web browser.

2.6. The CCIS must be capable of providing management information reports to meet the requirements of both national government and local needs.

2.7. The Council Corporate ICT Services (ICTS) will provide resilience of the server platform to ensure business continuity in the event of server failure based on the specification details provided.

2.8. The CCIS provider, the Council's ICT team and Corporate ICT Services will work closely together to ensure that:

2.8.1. Confidentiality protocols are in place
2.8.2. The CCIS is secure
2.8.3. A clear process is in place for data transfer arrangements particularly cohort data
2.8.4. Links are made between other key information sources

2.9. The CCIS must provide the scope for the development around CCIS (whilst maintaining national specification compliance) to meet the needs of the Council. This includes supporting work to establish interoperability with other systems (such as Microsoft Excel, Word and livechat) which exist currently or may be developed in future to enhance or improve the efficiency of service delivery, more effective data management, sharing and reporting.

2.10. Currently the client information is held in Cognisoft I O

3. CCIS Managed Service

3.1. The supplier will need to undertake the following functions;

3.1.1. Data migration of data to new CCIS platform if required
3.1.2. Provision of a CCIS compliant with the specifications and data catalogue provided by DfE.
3.1.3. Be a supplier with proven experience of managing CCIS and reporting to NCCIS
3.1.4. Management of all operations compliant with the GDPR
3.1.5. Managing data collection and exchange arrangements with all relevant providers including schools. colleges, private training providers and any other legitimate sources such as Individual Learner Record system and the Local Authority and neighbouring local authorities.
3.1.6. Bulk data processing

3.1.7. Help desk operations including fault reporting and resolution; support to staff and advice to managers regarding most up to date DfE requirements, and best practice in using the CCIS.
3.1.8. Monitoring of data for quality
3.1.9. Monthly meetings with Council staff for progress report and planning
3.1.10. Staff training for users including production of instructions for staff
3.1.11. MI dashboards to assist staff and managers to monitor progress against key KPIs and case load management, levels of contact
3.1.12. MI reporting to DfE meeting the requirements and time scales as stipulated in the current NCCIS Management Information Requirement published by DfE.
3.1.13. Provision of a Platform approved by DfE for CCIS
3.1.14. Share and exchange information between schools and the City of Wolverhampton Council to obtain;
3.1.14.1. Cohort data
3.1.14.2. Final cohort data
3.1.14.3. Conditional destination data
3.1.14.4. September offer data
3.1.14.5. Survey data
3.1.14.6. Risk of not engaging data
3.1.14.7. Missing destination data
3.1.14.8. September offers

3.2. There is a requirement to work with the Council to contribute to the development of local plans as it carries out its statutory duties. This will include providing any required data particularly relating to progression destinations of young people, intentions of young people relating to the September Guarantee, Destination Measures and local skill needs.

3.3. The System Provider will:

3.3.1. Identify a Project Manager responsible for initial roll-out.
3.3.2. Identify an Account Manager responsible for dealings with the Council.
3.3.3. Provide a project plan identifying milestones for implementation
3.3.4. Telephone support free of charge between the hours of 9am and 5pm, Monday to Friday.
3.3.5. Fault resolution and available for queries etc.
3.3.6. Identify restrictions on availability of support during the contract process.
3.3.7. Outline what support it would require from the Council to be able to meet the specification and timescales indicated.

4. Key Operational Areas

4.1. Key operational areas are set out below. The Provider must deliver the services required below, they are considered to be key operational areas and essential for the service.

4.1.1. Shared Database (scope for expansion for other systems e.g. One)
4.1.2. Web Access
4.1.3. Statistics – dashboard view of key KPI's or operation stats
4.1.4. Information export to other databases/data analysis (standard formats)
4.1.5. Case notes
4.1.6. Upload external docs (word, pdf, jpegs)
4.1.7. Timeline mapping of activities and events
4.1.8. Standardisation of information views
4.1.9. Customisable information (report) screens with filtering
4.1.10. Field Validation
4.1.11. Link in with corporate (LLPG/NLPG) gazetteer
4.1.12. Flexible to changes in central government policies
4.1.13. Levels of user record validation
4.1.14. High levels of activity auditing
4.1.15. Ability to confirm locations outside of the borough using a gazetteer
4.1.16. Create transfer files to share with other LA's
4.1.17. Capable of holding destination data
4.1.18. Ability to link into other systems such as Live chat and user portals
4.1.19. Data Quality monitoring
4.1.20. Notification of work actions/reviews – auto and local – work tray/flow
4.1.21. Customisable screens for user activity and data input
4.1.22. Personal caseload view (customisable homepage to create different views dependant on job role)
4.1.23. Calendar replication across case file areas (Single entry multiple postings)
4.1.24. In built messaging
4.1.25. Potential for synchronisation of internal calendar to Outlook
4.1.26. Potential to link to Corporate EDM
4.1.27. Potential to store a user photo for user identity confirmation
4.1.28. Case Notes
4.1.29. Chronology of all interactions and actions
4.1.30. Record of current status of client and provider,
4.1.31. Client characteristics including SEN, Vulnerable characteristics to meet reporting requirements
4.1.32. Record of referrals to other services
4.1.33. Record of other professionals involved
4.1.34. Facility to set up tasks and reminders of actions needed by case worker
4.1.35. Facility to attach documents to the client records
4.1.36. Differentiated level of access to sensitive information
4.1.37. Facility for caseworkers to set up case lists, filter searches by client characteristics, client's current status, or learning provider
4.1.38. Options for texting and emailing clients
4.1.39. Accessibility (Citrix compatibility)
4.1.40. Compatibility with current city of Wolverhampton council operating environments
4.1.41. Expandability options for cross LA sharing
4.1.42. Mobile device flexibility

5. Conditions of System

5.1. Where appropriate, compliance with the Government's Interoperability Framework (e-GIF) and Systems Interoperability Framework (SIF) is a requirement. These frameworks comprise of a number of technical policies, recommendations and standards. The Service Provider will be expected to identify its status in respect of these frameworks.

6. Costs

6.1. Details and costs need to be provided on the level of training required (on-site or off site) to cover the implementation and on-going use and support of the system. This needs to include how long the implementation will take and when it can start.

6.2. Details and costs need to be provided to indicate the frequency of updates and describe how these updates are applied to the running system indicating the amount of disruption to the service if any.

6.3. Itemise the deliverables included in the cost of the software licence (e.g. upgrades backups, email, telephone and/or onsite support for users, and the number of users including any upper limits). Costs for deliverables not included in the cost of the software licence should be itemised.

6.4. The System Provider will provide a full breakdown of costs.

7. Technical Requirements

7.1. Currently the client information is held in Cognisoft I O

7.2. The solution must be fully accessible and available for all registered users 99.95 of the time, 52 weeks per year to maintain the database.

7.3. The system must provide facilities for the restoring of information that has been lost or corrupted and must provide guarantees that a recovery can be performed, ensuring the integrity of the information.

7.4. It should be possible to produce backups of all data in a way that would allow the restoration of the system and its data to specific recovery points where the solution and data integrity is known to be intact.

7.5. First and second line support will be provided by the Council, however the Service Provider is required to detail the levels of service provided to support the Council in use of the system. The helpdesk service must provide support for the following:

7.5.1. Advice on how to operate the system.
7.5.2. Advice on potential ways to use the system to address a business need.
7.5.3. A point of contact for the notification of system errors/faults.
7.5.4. Investigation into the cause and effects of reported errors/faults.
7.5.5. Processes/Procedures to be undertaken by the user to resolve reported errors/faults.
7.5.6. Information on the current status of work being undertaken to resolve reported errors/faults.
7.5.7. Fixes to reported errors/faults in the form of system patches/upgrades/scripts.

7.6. The information displayed on any screen should be aligned with the working requirements of the user.

7.7. The solution should never allow data to be created in an inconsistent way or data to be left behind in case of unplanned ending of a transaction. The integrity of the data must be maintained at all times.

7.8. The solution must only lock records to prevent data integrity issues at the lowest level possible whilst maintaining data integrity.

7.9. The web based front end of the solution must be compatible with a range of the most widely used versions of the most popular web browsers. The minimum requirements in terms of browser compatibility are:

7.9.1. Internet Explorer version 6.0 and above.
7.9.2. Firefox 1.0 and above.
7.9.3. Google Chrome.

7.10. Suppliers should state whether the solution is reliant on users having browser technologies such as Java and Flash enabled for the web front end to operate correctly.

7.11. The solution should handle processes that encounter a problem in such a way as to maintain data integrity and must be able to terminate processes that encounter a problem without effecting overall performance. (Example: a process encounters a problem due to a service being unavailable, an error message should be generated, all data is returned to its original state and the user is permitted to continue to use the solution for processes that do not require that service).

7.12. The solution should terminate inactive sessions after a configurable predefined length of time.

7.13. The solution should require anyone wishing to access the system to login using an ID and password.

7.14. The solution should allow the system administrator to establish standards for the setting of user ID's and passwords. In order to achieve this, the solution should allow for the following:

7.15. Passwords length must be configurable (minimum and maximum length).
7.16. Passwords must contain at least a configurable number of the following character categories:
  7.16.1. Capital letters;
  7.16.2. Lower case letters;
  7.16.3. Numbers;
  7.16.4. Special characters.
7.17. Passwords may not contain more than a configurable number of identical sequenced characters from the old password. Passwords may not be repeated within a configurable number of changes.
7.18. A password change must be enforced by the system after the first login.
7.19. After a configurable time frame a password change must be enforced during the next login.
7.20. Passwords should not be displayed in plain text on the screen.
7.21. Ability for user/assessor to change their own passwords.
7.22. History of used passwords.
7.23. Expiration dates.
7.24. Restriction of re-use of passwords when expired.
7.25. Auto suspend user/assessor after a number of invalid logon attempts.

7.26. The solution must ensure that access to user/assessor ID and password information is controlled and restricted to appropriately authorised personnel.

7.27. The system must be capable of providing multiple levels of authorisation for access to the system. It must be possible to restrict users' access to the system in order to:

  7.27.1. Prevent user from viewing information that is confidential or is beyond their authority level for access.
  7.27.2. Prevent user from performing operations that they are not authorised
  7.27.3. to perform.
  7.27.4. Prevent accidental or malicious damage to the system or its data.
  7.27.5. Prevent user from altering data entered by others without a quality control mechanism for authentication being in place.

7.28. Audit reports should contain sufficient information to allow transactions of any sort to be traced end to end through the system.

7.29. The solution must be accessible and available for use to all users' and all assessors' at the same time without a reduction in performance. The solution must not limit the number of users' who can access the system at any one time.

7.30. Training must be available for users of the proposed solution. Suppliers must explain how training will be conducted, what training materials/operational manuals will be provided and what format these will be provided in (e.g. Printed, Electronic, on-line help etc.).

7.31. The solution must be capable of full operation on the existing desktop PC devices in use across the Council and their Connexions providers. The Council deploys client PCs to standard configurations, describe any issues that might arise from running your solution with the following:

7.31.1. Microsoft Systems Management Server agent.
7.31.2. Windows Management Instrumentation services.
7.31.3. Windows XP Service Pack 2.
7.31.4. Windows 7
7.31.5. McAfee Anti-Virus and encryption (laptop and desktop PCs)
7.31.6. Websense Security Enterprise Firewall protection

The list above is not intended to be exhaustive and is subject to change.

8. Reporting

8.1. Suppliers must confirm that as a minimum the system will produce the necessary reports required by DfE as stipulated in the NCCIS MI requirement and the Council. Listed below are the minimum reports required. Reports must be capable of being exported into Word, Excel and XML formats. The number of days required and costs for providing professional services in connection with your solution (e.g. custom report writing, data importing, and new features development) must be provided:-

8.1.1. NEET analysis by percentage (monthly, quarterly and annually).
8.1.2. Joiners and leavers.
8.1.3. Destinations.
8.1.4. Gender.
8.1.5. Duration (length of time NEET).
8.1.6. Ethnicity.
8.1.7. Location (NEET hotspots, ward).
8.1.8. EET (Employment, Education, Training) analysis.
8.1.9. Not known analysis.
8.1.10. Vulnerable groups including teenage mothers, young offenders, care leavers, alternative provision
8.1.11. 16-19 year olds with Special Education Needs and Disabilities (SEND).
8.1.12. 13-16 year olds with Special Education Needs and Disabilities (SEND).
8.1.13. Breakdown by type.
8.1.14. EHC (Education Health Care) completions.
8.1.15. Comparisons with national averages (to include Neighbourhood statistics).
8.1.16. Intended destinations from each May.
8.1.17. September Guarantee progress from each June.
8.1.18. Activity survey progress from each November.

8.1.19. Activity survey outcomes from end January.

8.2. Standard Reporting Requirements as stipulated by DfE and including:

8.2.1. NEET % analysis, monthly, quarterly annually
8.2.2. Not known % monthly, annually, quarterly
8.2.3. Joiners and Leavers
8.2.4. Destinations
8.2.5. September Offer progress from June
8.2.6. Activity Survey progress from November
8.2.7. Activity Survey Outcomes end January
8.2.8. Gender
8.2.9. Ethnicity
8.2.10. Location
8.2.11. EET analysis
8.2.12. Not known analysis
8.2.13. Vulnerable groups
8.2.14. 16-19 SEND
8.2.15. 13-16 SEND
8.2.16. Career Pathway Plan completions
8.2.17. Intended destination
8.2.18. Comparisons to national averages

9. Notifications

9.1. In relation to the Service the supplier shall notify the Council in writing within two Working Days or sooner of becoming aware of any of the following circumstances:

9.1.1. Investigation and outcome of any Safeguarding Adults investigation
9.1.2. Whistle blowing or any incident in connection with whistle blowing
9.1.3. Changes to agreed staffing levels
9.1.4. Change of Nominated Contact Person
9.1.5. Any underperformance including service usage against agreed levels
9.1.6. The Provider organisation enters into an agreement to deliver additional service(s) and/or activities which may impact upon its capacity to deliver the service(s) specified within this Contract
9.1.7. Change of title address telephone fax email of Nominated Contact Person
9.1.8. Death of a Service User or any other serious incident or accident
9.1.9. Outbreak of any infectious disease which in the opinion of a registered medical practitioner is sufficiently serious to be so notified
9.1.10. Any serious complaint/allegation made against the Provider or a member of staff
9.1.11. Landlord serves notice on a lease
9.1.12. Changes to Service Users circumstances that may affect either their entitlement to benefits and/or their ability to pay charges

9.1.13. Change in who controls the majority of shares in or the voting rights amongst shareholders of members of the Providers organisation or there is a material change in the objects of the organisation
9.1.14. The Provider organisation merges with another organisation
9.1.15. The Provider organisation in any way transfers its business to another organisation
9.1.16. As a result of any misconduct or mismanagement on the part of the Provider organisation an official or regulatory body directs an inquiry into or makes an order of any kind in relation to the Provider organisation
9.1.17. Any statutory or other registration which the Provider organisation must maintain in order to provide any service is withdrawn cancelled or is threatened to be withdrawn or cancelled
9.1.18. The Provider organisation is required to have and is awarded any statutory or other registration in order to provide any services
9.1.19. Any placing and/or lifting of any notice by a regulatory body
9.1.20. Any action being taken and/or pending in respect of alleged breach and or non-compliance to Equal Opportunities
9.1.21. Any dispute relating to this Contract or its delivery

(NB this list is not exhaustive)

10. Commercial

10.1. Maintenance Services will be charged from the date of acceptance of the system 'Go-Live' date and will be payable annually in advance during the life of the contract, not upon signature of the agreement.
10.2. The CCIS must be compliant with the specification and data catalogue drawn up by DfE and be capable of electronic submissions to the DfE/NCCIS portal. The Supplier must keep the CCIS compliant with all existing, amended and new statutory requirements of the DfE/NCCIS.
10.3. Any changes to the CCIS as a result of DfE amendments should be reflected in system upgrades (at no cost to the Council) and made in line with any deadlines imposed by such DfE changes.
10.4. Due to restrictive budgets the Council reserves the right to review on an annual basis the number of licences and reduce as required.
10.5. There should be a minimum of 5 years left in the life cycle of the proposed CCIS and full support for a minimum of 5 years.
10.6. Upon completion of the contract any data held by the Supplier or subcontractor during the contract term will need to be provided back to the Council free of charge in an agreeable format.