CITY OF WOLVERHAMPTON COUNCIL

Response to Request for Information

Reference FOI 002554
Date 19 July 2018

Tracking Young People

Request:

I am emailing to make a request under the Freedom of Information Act 2000 for information regarding your authority's services for tracking young people, support for those who are NEET and not Participating and the approach you take to meet your statutory duties under The Education and Skills Act 2008, the Duty to Participate and in line with the DfE NCCIS requirements.

Please can you answer the following questions?

1. Does the Local Authority provide the CCIS and Tracking Services or is this contracted out?
   The CCIS service is contracted out. Tracking of those not participating is done jointly by the contractor and Connexions.

2. If the service is contracted out can you please:

   a) Indicate the name of the service provider;
   b) Please provide a copy of the service specifications issued and the winning tender responses;
   In response to questions 2a) and 2b) above, please find attached information.

   c) Indicate the contract value.
   Value of the CCIS data management element is £61,829.04.

3. Which CCIS System is used? Please indicate the name of the Vendor/System Supplier and whether this is hosted by the Local Authority or by the Software Supplier.
   Cognisoft IO.
   This is hosted externally but not with the software supplier.

4. How Many Staff are employed in;

   a) Supporting and Running the CCIS System;
   1.1

   b) Undertaking the Tracking and Follow Up function.
   0.5 contractor and approximately 3.5 Connexions delivery staff and Connexions management time approximately .2

5. What are the costs associated with/value of the contract for providing these services?
   £61,829.04

Schedule A: Specification

1.1 This procurement is for the provision of a managed Connexions Client Caseload Information System (CCIS) that must be operational on 1st October 2015. The service will provide full implementation of the system including management, on-going maintenance, training, data migration and cleansing and report production as specified.

1.2 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 on NCCIS is used to:

- 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.
- Produce monthly tables which are available on the NCCIS portal for services to compare and benchmark their performance against others.
- 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.
- Combine with other administrative data to produce KS4 and KS5 destination measures and the NEET Quarterly Brief.

1.3 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 Wolverhampton Connexions Service.

1.4 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. The system and the management of it must be compliant with the requirements of the Data Protection Act.

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

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

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

1.8 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.

1.9 The system provider, the Council's Children's Services Strategic ICT team and Corporate ICT Services will work closely together to ensure that:

- Confidentiality protocols are in place
- The system is secure

- A clear process is in place for data transfer arrangements particularly cohort data
- Links are made between other key information sources

1.10 The system 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 One, Microsoft Excel, Access, 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.

1.11 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.

1.12 Currently the client information is held in Profile – 2000 and the existing data will need to be imported into any new system.

1.13 The System Provider will:

a) Identify a Project Manager responsible for initial roll-out.
b) Identify an Account Manager responsible for dealings with the Council.
c) Detail what level of support is available during the implementation stage.
d) Detail what level of support is available on an on-going basis. For example is telephone support free of charge, at what cost, what hours are covered?
e) Detail if the support is only for fault resolution or available for queries etc.
f) Detail any restrictions on availability of support.
g) Outline what support it would require from the Council to be able to meet the specification and timescales indicated.

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

Key Operational Area
System Requirements
Shared Database (scope for expansion for other systems e.g. One
Web Access
Statistics – dashboard view of key KPI's or operation stats
Information export to other databases/data analysis (standard formats)
Case notes
Upload external docs via scanning
Timeline mapping of activities and events
Standardisation of information views
Customisable information (report) screens with filtering
Field Validation
Link in with corporate (LLPG/NLPG) gazetteer
Flexible to changes in central government policies
Levels of user record validation
High levels of activity auditing
Ability to confirm locations outside of the borough using a gazetteer
Create transfer files to share with other LA's

Capable of holding destination data
Ability to link into other systems such as Live chat and user portals
Data Quality monitoring
Notification of work actions/reviews – auto and local – work tray/flow
Customisable screens for user activity and data input
Personal caseload view (customisable homepage to create different views dependant on job role)
Calendar replication across case file areas (Single entry multiple postings)
In built messaging
Potential for synchronisation of internal calendar to Outlook
Potential to link to Corporate EDM
Potential to store a user photo for user identity confirmation
Technical Requirements
Connexions Technical Specification
Connexions Statutory requirements
Reporting tool requirements
Accessibility (Citrix compatibility)
Compatibility with current SMBC operating environments
Expandability options for cross LA sharing
Mobile device flexibility

2. Conditions of System

2.1 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.

2.2. **System**

The System Supplier must complete the Detailed System Response questions in outlined in the Award Criteria.

2.3. General

(a) 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.

(b) 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.

(c) 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.

(d) The System Provider will provide a full breakdown of costs.

3. Detailed System Response

3.1 Data Migration

Currently the client information is held in Profile – 2000 and the existing data will need to be imported into any new system.

3.2 System Availability

The solution must be fully accessible and available for all registered users between the hours of 07:00hrs and 20.00hrs Monday to Friday and between 07.00hrs and 15.00hrs on Saturdays x 52 weeks per year to maintain the database.

3.3 Recovery of Lost Data

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.

3.4 Backup Strategy

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.

3.5 Helpdesk Responsibilities

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:

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

3.6 Restrict Information Displayed

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

3.7 Data Integrity

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.

3.8 Record locking

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

3.9 Browser Compatibility

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:

- Internet Explorer version 6.0 and above.
- Firefox 1.0 and above.
- Google Chrome.

3.10 Browser Technologies

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.

3.11 Handling of Frozen Processes

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).

3.12 Inactive Sessions

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

3.13 System Access

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

3.14 Password Standards

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:

- Passwords length must be configurable (minimum and maximum length).
- Passwords must contain at least a configurable number of the following character categories:
  - Capital letters;
  - Lower case letters;
  - Numbers;
  - Special characters.
- 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.

- A password change must be enforced by the system after the first login.
- After a configurable time frame a password change must be enforced during the next login.
- Passwords should not be displayed in plain text on the screen.
- Ability for user/assessor to change their own passwords.
- History of used passwords.
- Expiration dates.
- Restriction of re-use of passwords when expired.
- Auto suspend user/assessor after a number of invalid logon attempts.

3.15 Access To User ID's and Passwords

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

3.16 Access Levels

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:

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

3.17 Audit Reporting

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

3.18 Concurrent Access

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.

3.19 Training of Users

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.).

3.20 Desktop Devices

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:

- Microsoft Systems Management Server agent.
- Windows Management Instrumentation services.
- Windows XP Service Pack 2.

- Windows 7
- McAfee Anti-Virus and encryption (laptop and desktop PCs)
- Websense Security Enterprise Firewall protection

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

3.21 Reporting

Suppliers must confirm that as a minimum the system will produce the necessary reports required for 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:-

- NEET analysis by percentage (monthly, quarterly and annually).
- Joiners and leavers.
- Destinations.
- Gender.
- Duration (length of time NEET).
- Ethnicity.
- Location (NEET hotspots, ward).
- EET (Employment, Education, Training) analysis.
- Not known analysis.
- Vulnerable groups including teenage mothers, young offenders, care leavers
- 16-19 year olds with Special Education Needs and Disabilities (SEND).
- 13-16 year olds with Special Education Needs and Disabilities (SEND).
- Breakdown by type.
- EHC (Education Health Care) completions.
- Comparisons with national averages (to include Neighbourhood statistics).
- Intended destinations from each May.
- September Guarantee progress from each June.
- Activity survey progress from each November.
- Activity survey outcomes from end January.