St Helens Council – Income Management / Payment Processing System

St Helens Council is reviewing its incumbent Income Management / Credit / Debit Card payment system with a view to reducing the Council's scope to testing and compliance under the Security Standards Council requirements for Payment Card Industry Data Security Standards (PCI DSS). The support contract for the current system is due to expire ion *.

As part of the review process, the Council wishes to undertake market testing around possible replacement solutions and services. As such, the Council requires solutions which offer the latest payment options to its customer's i.e. Internet, contactless and mobile payments etc. ensuring there is no security risk to the Council or its customers. These will need to run alongside existing payment channels such as face to face and IVR (integrated voice recognition).

The system must be able to also process cash, cheque, bank credits, fund transfers and batch processing.

The system will need to cater for a number of imports e.g. Bank Files, DWP Files, importing of schedules from Debt Collection Agencies, along with suspense clearance functionality. The system will also need to integrate with external software; currently St Helens has payment integration with XN Leisure and Lalpac (Idox).

A comprehensive reporting suite is required to facilitate the cash reconciliation process and the system will need to produce a cash end of day file in a specified format to feed the Council's main financial information system.

The Council is already progressing PCI compliant solutions around call recording within its Contact Centre and telephony infrastructure.

It is envisaged any replacement system and services will be hosted or cloud based. This is in line with the Council's strategy of a cloud first approach for replacement or new systems.

The Council will be looking to hold supplier briefing days at which an overview and demonstration of their system will take place. The session must clearly demonstrate the functionality mentioned above, including each of the payment channels and their positioning and integration within a card holder data environment. A clear explanation and evidence of reduced PCI DSS compliance provided by the solution and services must also be presented.