16.2. The Service Provider shall close/suspend a subscription associated with a Customer Online Account, in accordance with process document (Close/suspend Customer subscription) of Appendix 1 (Process Document Register), when at least one of the following occurs:

16.2.1. the Customer gives the Service Provider notice to close the subscription if there is no outstanding debt;

16.2.2. authorised Authority Personnel instructs the Service Provider to close/suspend the subscription; and

16.2.3. a Customer's annual subscription expires and the Customer cannot be contacted via any of the contact channels provided.

17. Fraud and Suspicious Activities

17.1. The Authority undertakes regular checks on fraudulent and suspicious activities. The Service Provider shall assist the Authority on any investigation into fraud or suspicious activities.

17.2. The Service Provider shall maintain a log of suspicious activities and shall make this log available to the Authority upon request.

17.3. The Authority shall provide, and the Service Provider shall comply with, guidelines for investigating irregular or suspicious activity where the cases are in relation to the Service Provider Personnel.

17.4. The Authority shall provide any evidence of irregular activity identified in the Authority's systems and applications to the Service Provider for full investigation. The outcome of the Service Provider's investigation shall be sent to the Authority within 10 Business Days of the Authority providing the evidence. The Service Provider shall review such evidence on a case by case basis and will promptly agree a course of action with the Authority's Internal Audit Department and the Service Provider to correct the irregular activity and prevent the reoccurrence of the irregular activity.

18. Quality Audits

18.1. The Authority shall undertake Periodic quality and compliance to LCHS process audits on the Agents. In addition to this, the Authority shall also perform quality and compliance audits on the Agents through an independent third party.

18.2. The audit assessments shall be based on the criteria detailed in Appendix 5 (Quality Measurement Criteria). The Agents shall be measured against the criteria set by the Authority and the criteria set by Top 50 Mystery Shopper Survey.

18.3. The Authority and the Service Provider will review the results of the audits, discuss and plan for actions for resolving any ongoing issues at the Service Review Meeting every Period to be implemented at the Service Provider's cost.

19. Secure Disposal

19.1. Disposal of materials, including all personal Data (as applicable), must be carried out at the Service Provider's premises using crosscut shredding equipment, or other secure disposal method approved by the Authority.

19.2. The sub-contractor, if any, used for this process, must be approved by the Authority fraud and security department.

20. Data Retention

20.1. The Service Provider shall retain and dispose of all Data, including Personal Data, in accordance with Clause 24 (Records, Audit and Inspection).

20.2. Data retention rules may be changed by the Authority from time to time.

21. Security

21.1. The Service Provider shall ensure that any premises to be used to deliver the Services, will adopt such physical security measures, as Assured by the Authority, to reduce the risks of any criminal, or other, activity to the detriment of the Authority, to an agreed level, as low as reasonably practicable.

21.2. The Service Provider shall have and maintain written practices and procedures, to be approved by the Authority. These will include but not be limited to:

21.2.1. levels of logical security to be applied and maintained in order to protect the software process, such that 'end to end' security of the process is achieved. Access and password levels shall be devised for Service Provider Personnel, with any attempt at unauthorised access being referred automatically to management, with a distinct transaction audit trail being maintained;

21.2.2. physical security, including intruder detection;

21.2.3. fire prevention/detection; and

21.2.4. actions to be taken to suspend and/or investigate any Service Provider Personnel or site suspected of aiding fraudulent and/or criminal activity or aiding a breach of security.

21.3. The Service Provider shall demonstrate that these policies, systems and processes have been designed to comply with BS7799 (Part 1)/ ISO/IEC 27001, PCI DSS Level 1 and any other industry best practice that may be issued from time to time.

21.4. The Service Provider shall ensure Service Provider Personnel have undertaken Disclosure and Barring Service in England ("**DBS**") or Basic Disclosure Scotland in Scotland ("**BDS**") checks before providing any of the Services under the Contract, and as directed by the Authority.

21.5. Pursuant to Clause 24 (Records, audits and inspection) the Authority reserves the right to conduct audit checks on DBS or BDS certificates annually or at such other time as may be reasonably required by the Authority. The Service Provider shall maintain and provide a report containing a list of all Service Provider Personnel requiring access to the Authority's systems and applications on a Periodic basis.

21.6. The Service Provider will take all possible steps to limit the potential for loss or misuse of any Authority Assets. The Service Provider shall be responsible for any losses caused by fraud, misuse, negligence or wilful default by Service Provider Personnel.

22. Payment processing and accounting

22.1. The Service Provider shall be Payment Card Industry Data Security Standard ("**PCI-DSS**") Level 1 compliant and will ensure that they act in a PCI-DSS Level 1 compliant manner. Pursuant to Clause 30.12, the Service Provider shall:

22.1.1. Inform the Authority within 24 hours, if the Service Provider should suffer a payment card Data breach.

22.1.2. Provide a plan within 30 days for remediation, should the Service Provider fall out of PCI-DDS Level 1 compliance. Failure to maintain Level 1 compliance may result in termination at the Authority's discretion.

22.2. The Service Provider shall be liable for any costs arising and penalties issued by the card schemes (Visa, MasterCard, American Express) in relation to non-compliance with the PCI-DSS standard.

22.3. Payment cards are to be processed using the Authority's merchant acquirer as appointed from time to time. All transactions shall be authorised online and shall utilise Address Verification System ("**AVS**") and Card Verification Value ("**CV2**") security code verifications. Transaction charges shall be borne by the Authority.

22.4. The Service Provider shall accept only Amex, Electron, Maestro, MasterCard and Visa payment cards.

22.5. All payment card transactions are to be authorised and cleared prior to issuing any Associated Tokens. Any failure to carry out this requirement will be at the cost of the Service Provider.

APPENDIX 1 - PROCESS DOCUMENT REGISTER

As at the date of the Contract

Process Ref	Title	Version No.
LCHS_1	Activating Customer Key	V0.2
LCHS_2	Business Account to standard Customer account	V0.1
LCHS_3	Create Customer Online Account	V0.1
LCHS_4	Create Customer Record in CRM	V0.2
LCHS_5	Creating Business Account	V0.1
LCHS_6	Cycle cannot be docked	V0.2
LCHS_7	Deactivating Customer Online Account	V0.2
LCHS_8	Extend Customer journey/Docking Station locator	V0.2
LCHS_9	Handle insurance claim query	V0.1
LCHS_10	Identification and verification	V0.1
LCHS_11	Investigate charging issue	V0.2
LCHS_12	Log Key lost, stolen or faulty	V0.2
LCHS_13	Cycle lost, stolen or faulty	V0.1
LCHS_14	Manage Customer Payment card	V0.2
LCHS_15	Manage handling Plan calls	V0.1
LCHS_16	Process refunds requests	V0.1
LCHS_17	Produce Promo Codes (external request)	V0.1
LCHS_18	Provide scheme information	V0.2
LCHS_19	Purchase Bike Access Period	V0.2
LCHS_20	Reactivate Customer Online Account	V0.1
LCHS_21	Reset Customer Online Account password	V0.2
LCHS_22	SM_Authorised charge	V0.2
LCHS_23	SM_Debt collection notifications	V0.1
LCHS_24	SM_Escalate to TfL	V0.2
LCHS_25	Fulfil Key request	V0.2
LCHS_26	SM_Handling undelivered mail	V3
LCHS_27	SM_Key stock management	V0.1
LCHS_28	SM_Late return charge	V0.1
LCHS_29	SM_Manage cheque/postal order payments	V0.2
LCHS_30	SM_Processing Chargebacks	V0.1
LCHS_31	SM_Produce Promo Codes (internal request)	V0.1
LCHS_32	Statement request	V0.2
LCHS_33	Third Party Incident Communication	V0.1
LCHS_34	Triaging Third Party Incident (CRM solution)	V0.1
LCHS_35	Triaging Third Party Incident (Telephone)	V0.1
LCHS_36	Update Customer Online Account Information	V0.1
LCHS_37	Update Customer Record in CRM	V0.1

APPENDIX 2 - Contact Centre Systems and Application Specification

1. Microsoft Dynamics Customer Relationship Management (MSD CRM)
2. TfL Online(for TfL Docking Station Availability Map)
3. Distributed Back Office System (DBOS)
4. TFL Knowledge Base (currently SharePoint)

1. Microsoft Dynamics Customer Relationship Management (MSD CRM)

Overview

MSD CRM is used to manage and record all Customer interactions. Each Contact can be recorded as either a Service Ticket, or a Customer Record can be set up if this does not already exist and the contact recorded via a Service Ticket for the Customer Record. The Service Tickets numbers generated via MSD CRM are also used in various other systems as a reference against any information stored. Service Tickets can be created via various means of Contact; telephone, email, web form, fax and letter. These are all viewable within MSD CRM and attached to the relevant Service Tickets.

Customer Record contain the Customers full name; address; telephone number; and email address. They also contain any documentation or emails sent in via the Customer. If any Service Tickets are found to contain any financial information, they can be marked as sensitive which prevents any personnel without the appropriate permission from viewing that Service Ticket.

MSD CRM is a cloud based solution, hosted by the Authority.

MSD CRM is accessed via a URL.

User credential management

This will be managed by the Authority

Licenses

Service Provider to propose the number of licenses required, for the Authority to agree, as part of Transition

2. TfL Online

Overview

TfL Online is a web based application accessible to the public, which is used by Agents to locate and map bike docking station information to Customers.

Application steps

1. Access the link https://tfl.gov.uk/maps/cycle-hire
2. Enter the Customers current location details (postcode, address, station, stop or pier)

3. A list of docking stations in the area will be shown, with the closest at the top.
4. The number of bikes and spaces available is shown in the list view.
5. Click on a different docking station (if needed) to find its location to direct the Customer.

User credential management

No user credentials or management required as it is a public facing website,

Licenses

No licensing cost or max concurrency as public facing website.

3. Distributed Back Office System (DBOS)

Overview

DBOS is the back office system for the Cycle Hire scheme. It manages a Customer's accounts, payment, billing, bike hires, physical assets such as bikes, keys and terminals including Docking Points. The DBOS system can be administered through the DBOS Management Console. This is a web based user interface which can be used to view status of customers, journey and payment history. It can also be used to associate keys to customer accounts which can then be sent out to customers. Payments can also be made through the DBOS Management Console.

User credential management

This will be managed by the RCC Contractor and the Authority.

Licenses

No licensing cost or max concurrency to need to comment on.

4. TfL Knowledge Base (currently SharePoint)

Overview

SharePoint is a web based application that is used to share information and knowledge. The section of SharePoint that is used primarily by Agents is the knowledge base. The knowledge base is regularly updated with process changes, upcoming events and pertinent ticketing bulletins. This is maintained by Authority's knowledge team and will include all previously used Cycle Hire documentation and information.

Application Steps;

1. Enter http://onelink.tfl.gov.uk/sites/custex/ccokb/Pages/KnowledgeBase.aspx in internet explorer.

User Credential Management

This will be managed by the Authority

Licenses

None

APPENDIX 3 - Historic demand

Historic demand profiles are included in the attached file which shall be provided to the Service Provider in electronic format before Contract Commencement Date.

S4 A3 CH Historic
Demandv0.3.xlsx

APPENDIX 4 - Reporting Requirements

1. Running total of “weekly” reporting shall commence from Sunday to Saturday
2. Running total of Periodic reporting shall commence from the 1st day of the reporting Period
3. All reporting shall be shown against any applicable targets set in Appendix 1 (Service Levels) of Schedule 8 (Service Management)

Report type	Key performance indicators included in report
Daily at 10:00	All reporting for the previous day: **Call Handling** • Forecasted calls (per hour and for the day). • Calls offered (per hour and for the day). • Calls answered (per hour and for the day). • Call abandonment rate percentage (per hour and for the day). • Maximum queue time for the day. • Number of call transfers to the Authority’s contact centre and other Third Party contact centres (running total for the week and the Period). • Number of call transfers to the Service Provider (running total for the week and the Period). • Average time to answer calls (hourly, daily and running Periodic total), • Average Talk Time for LCHS calls (hourly, daily and running Periodic total). • Staff absence figures for the day (including sick, duty sick, unplanned leave, other absent) by FTE and in hours. **Correspondence** • Total number of LCHS correspondences closed in reported day, categorised by the number of days taken to close the Service Ticket outside of the target. **Key Fulfilment** • Key Fulfilment daily totals for Associated Token orders (number of open orders categorised by Welcome Pack type and number of days it has taken to fulfil them). **General** • Commentary to explain any key trends, anomalies, Service Level breaches, or points of interest.
Weekly on Monday at 10:00	All reporting for the previous week (Sunday to Saturday): **Call Handling** • Forecasted calls (per day and for the week). • Calls offered (per day and for the week). • Calls answered (per day and for the week). • Call abandonment rate percentage (per day and for the week). • Maximum queue time (per day and for the week).