MEASURED TERMS AGREEMENT

between

and

Saltash Town Council, (the "Client")
whose registered office address is: xxx

Version: 1.1
Date: December 2021

INTRODUCTION

This contract sets out the IT support service to be provided by to Saltash Town Council during the period commencing on 1st April 2022 and terminating on 31st March 2024.

SERVICE SPECIFICATION

1.0 Service Includes

1.1 Ongoing support of all computer workstations (excluding hardware support), network operating systems, mail systems and Microsoft Office Suite.

1.2 The provision of for reporting all ICT related incidents and obtaining information on service status and matters associated with any reported incident. This includes the logging, monitoring and escalation (where appropriate) of all incidents reported to the HelpDesk. The work resulting from any logged request is dealt with in Section 2.

1.3 The provision of advice and assistance to identify suitable IT and Telecomms products in response to a need expressed by the Client. Requests for such assistance will be introduced as a request for support under the procedure outlined in section 4.0.

2.0 Service Delivery

2.1 The Service will be for up to 3.5 on-site hours and up to 4 remote support/maintenance hours per calendar month during the period Monday to Friday excluding public or national holidays.

2.2 The Service will be delivered in the main by a team of Technical Support Analysts with the back up of additional Technical Support, Communication and Networking Analysts where necessary from Services team.

2.3 The Technical staff will acknowledge requests for ICT Support and fault calls, normally within 8 working hours.

2.4 When appropriate and in order to provide a more efficient and rapid response, the Technical staff will resolve faults and satisfy requests by issuing instructions to the Client via telephone or e-mail.

2.5 Depending on the urgency of the logged call when an on-site visit, i.e. to the Client's registered office address, is necessary to resolve a fault or satisfy a request, the visit will normally be made within 3 working days of receipt of logged call.

2.6 Revised or new ICT policy will be recommended where appropriate and directed to the Client for consideration. Where recommendations are to be actioned and require an IT resource to implement any aspect, these must be introduced as requests for additional services as described in paragraph 3.3 below.

3.0 Service Exclusions

3.1 The supply or maintenance of any items deemed by the manufacturer to be consumable i.e. ribbons, floppy disks, toner, drums, fusers, filters, printheads, CRT's etc.

3.2 The hardware maintenance of all servers, computers and associated networking equipment and cabling, workstation hardware and printers.

3.3 Requests for support, which fall outside the service specified in 1.0 above can still be made to the HelpDesk (within the working parameters outlined in Section 2) and will be considered as a request for additional support. Charges for resulting work will be agreed in advance of the work being undertaken.

4.0 Call Logging Procedure

4.1 All faults or requests for IT support should be logged with the HelpDesk or via e-mail to the HelpDesk The Client in each case should provide a realistic priority of any logged call.

4.2 All relevant details about the fault or request must to be given to the HelpDesk operator as appropriate. All requests will be logged with the HelpDesk so that service delivery can be monitored.

4.3 Serious issues, escalations and complaints should be directed at the earliest opportunity to Director, either by phone call or via e-mail.

TERMS AND CONDITIONS

5.0 Costs

5.1 The cost for the provision of the Service specified in Section 1.0 above for the period from 1st April 2022 to 31st March 2024 inclusive is £240.00 per calendar month. On the 1st January each year, the contract value will increase in line with RPI.

5.2 The hourly fee will then be at £60 per hour.

This hourly charge will also be levied when it is necessary to either work off or to take work off-site, e.g. to offices, to resolve the problem

5.3 All reasonable expenses incurred by the Technical support staff, whilst carrying out any duties as part of this agreement, will be re-charged to the Client at cost, e.g. parking, and mileage will be charged at the rate of 50p per mile. Mileage expenses for contracted days at the head office are included in the daily rate.

5.4 All charges will be invoiced in arrears. Invoices will be addressed to Accounts Dept., at the address shown on the front page, unless is instructed otherwise.

All costs quoted above are ex VAT.

5.5 Data Protection

- The Contractor shall duly observe all its obligations under the General Data Protection Regulation 2018 ("the GDPR") in connection with the Service and this Agreement and shall ensure that the Client shall not be in breach of its obligations under the GDPA as a result of any act or omission of the Contractor. The Contractor shall not:
    - Use the data or information nor reproduce the data or information in whole or in part in any form except with the prior written agreement; or
    - Disclose the data or information to any third party or persons not authorised by the Client to receive it, except with the prior written consent of the Client; or
    - Alter, delete, add to or otherwise interfere with the data or information (save where expressly required to do so by the client to perform maintenance/operations on the ICT system).
- To the extent that any data or information relating to the Client, its staff and customers is personal data.
- The Contractor will not transmit such data and information to a country or territory outside the European Economic Area without the Client's express consent; and
- The Contractor will take such technical and organisation measures (5.6) against unauthorised or unlawful processing of such data and information and again accidental loss or destruction of, or damage to, such data and information as are appropriate to the Client as data controller.
  The Contractor shall indemnify the Client in full respect of any claims, proceedings, actions, damages, legal costs, expenses and other liabilities arising from the breach of this Condition by the Contractor

5.6 Organisational Data Protection Measures

- Should the contractor ever be required to take data from the clients site, it will be in an encrypted form, and the contractor will ensure that it's a secondary copy (i.e. There will be another backup) of the data before leaving site.
- All e-mails between the contractor and the client are encrypted via TLS.
- All documents stored by the contractor are held in an encrypted format and/or require 2FA (2nd factor authentication) to access them.

5.7.1 Organisational Security Measures

Security Management

a. Security policy and procedures: Contractor **(Processor)** must document a security policy regarding the processing of personal data.

b. Roles and responsibilities :

i. Roles and responsibilities related to the processing of personal data are clearly defined and allocated in accordance with the security policy.

ii. During internal reorganisations or terminations and change of employment, revocation of rights and responsibilities with respective handover procedures is clearly defined.

c. Access Control Policy: Specific access control rights are allocated to each role involved in the processing of personal data, following the need-to-know principle.

Incident response and business continuity

a. Incidents handling / Personal data breaches:

   i. Processor will report without undue delay to Controller any security incident that has resulted in a loss, misuse or unauthorised acquisition of any personal data.

b. Business continuity: Processor establishes the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach).

Human resources

a. Confidentiality of personnel: Processor ensures that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities are clearly communicated during the pre-employment and/or induction process.

b. Training: Processor ensures that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data are also properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.

Technical security measures

Access control and authentication

a. An access control system applicable to all users accessing the IT system is implemented. The system allows creating, approving, reviewing and deleting user accounts.

b. When granting access or assigning user roles, the "need-to-know principle" shall be observed in order to limit the number of users having access to personal data only to those who require it for achieving the Processor's processing purposes.

c. Where authentication mechanisms are based on passwords, Processor requires the password to be at least eight characters long and conform to very strong password control parameters including length, character complexity, and non-repeatability.

d. The authentication credentials (such as user ID and password) shall never be transmitted unprotected over the network.

Security of data at rest

a. Server/Database security

   i. Database and applications servers only process the personal data that are actually needed to be processed in order to achieve its processing purposes.

b. Workstation security:

   i. Users are not able to deactivate or bypass security settings.

   ii. Anti-virus applications are configured on a regular basis.

iii. Users don't have privileges to install or deactivate unauthorised software applications.

iv. The system has session time-outs when the user has not been active for a certain period.

v. Critical security updates released by the operating system developer are installed regularly.

Network/Communication security:

a. Whenever access is performed through the Internet, communication is encrypted through cryptographic protocols.

b. Traffic to and from the IT system is monitored and controlled through Firewalls and Intrusion Detection Systems.

Back-ups:

a. Backup and data restore procedures are defined, documented and clearly linked to roles and responsibilities.

b. Backups are given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.

c. Execution of backups is monitored to ensure completeness.

Mobile/Portable devices:

a. Mobile and portable device management procedures are defined and documented establishing clear rules for their proper use.

b. Mobile devices that can access the information system are pre-registered and pre-authorised.

Data deletion/disposal:

a. Software-based overwriting will be performed on media prior to their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction will be performed.

b. Shredding of paper and portable media used to store personal data is carried out.

Physical security: The physical perimeter of the IT system infrastructure is not accessible by unauthorised personnel. Appropriate technical measures (e.g. Intrusion detection system, locking system) or Organisational measures (e.g., security guard) shall be set in place to protect security areas and their access points against entry by unauthorised persons.

6.0 Personnel

6.1 The personnel provided by will remain under the control of Neither nor the Client shall solicit the services of or employ or otherwise contract for the services of any present or future employee of the other without the consent of the other until 6 months after the earlier of (a) the termination of such employee's employment or contract, or (b) the termination of this Agreement

7.0 Review and reporting

7.1 A director of will be available to meet on a regular basis (to be agreed with the Client) to discuss any service issues or any new requirements, in order to ensure optimal value for money is being derived from this contract.

7.2 The Client will be responsible at all times for all ICT policy and procedures. Ltd. will advise the Client, as appropriate, where there is an apparent need to change or add any policy or procedures where they will be of benefit to the Client.

8.0 Termination

8.1 This contract may be terminated by either party for whatever reason by giving the other 90 days written notice.

AGREEMENT

By signing this contract you are formally indicating your agreement to the terms and conditions detailed in this document.

Signed: _____ Date: _____
For and on behalf of Saltash Town Council

Name (please print): _____

Position: _____

Signed: _____ _____ Date: __1st April 2022_____

Name (please print):

Position_____Director_____