



Looe Town Council Tender for IT Services

Introduction

Looe Town Council is seeking a provider to deliver and manage the IT services used by the Council staff and elected Councillors. The support will be considered for approximately 12 staff and 15 Councillors. Staff work both at the Council offices in Looe and remotely. Councillors are part-time, generally use their own devices and attend the Council offices and other locations for meetings.

All responses should make clear statements about the following support areas:

- Remote and physical support to staff hardware and application needs
- Secure cloud data management
- Flexible remote access for staff and Councillors
- Data protection compliance, including GDR
- The replacement of local data backups with an automated continuity solution
- Physical IP network design changes to ensure cost effective continuity based on the infrastructure available now or within 3 years.

Key Tender Requirements to Include

1. Microsoft 365 Cloud Management

- **License Management:** Suppliers shall propose a solution that permits different classes of users to be configured in the most cost-effective way. It is expected that the solution will include a mix of licence types for staff and potentially Microsoft 365 Frontline Worker (F-Series) licenses for Councillors.
- **Identity and Access Management:** The proposed solution shall implement strict control over who can access council files, ensuring former councillors or staff have their access immediately revoked. The solution shall review the existing SharePoint sites and recommend a restricted SharePoint structure.
- **User account:** The proposed solution shall ensure all admin and superadmin passwords are held securely by the Proper Officer (or deputy) within the Council as well as by the provider.
- **Device Management:** The solution shall propose and implement Mobile Device Management (MDM) to protect council data on personal or shared laptops/phones used

by Councillors and staff. It is expected that the proposed solution shall ensure compliance with Microsoft Eligibility and Enterprise Mobility + Security.

2. Cybersecurity & Data Compliance

- **UK GDPR Compliance:** The council handles sensitive public data. The proposed solution shall ensure all systems (including home-working devices and Councillor devices) meet current regulations.
- **Endpoint Protection:** The IT support solution shall ensure that Antivirus and ransomware protection is installed and managed on all staff devices, with automated patching for Antivirus and MS products where practical. The cost for ensuring all patching is carried out shall be included in the tender response.
- **Cyber Essentials Accreditation:** All tender responders shall provide evidence that they are certified under the UK Government's Cyber Essentials Scheme.

3. Backups & Disaster Recovery

- **Cloud-First Backup:** The solution shall remove the need for any local hard drive to avoid the physical security risk (theft, fire, or hardware failure). The solution shall implement a cloud-based backup (e.g., Azure or Microsoft 365 backup) for all documents and emails.
- **Disaster Recovery Plan:** The solution proposed shall clearly define the protocol for how quickly data can be restored if systems go down. It is desirable that, in the event of local system failure, remote working can continue. All systems shall be restored in a reasonable time, considering the business needs of the Council.

4. Remote & Flexible Support

- **Helpdesk Availability:** Helpdesk support hours must cover the times given in the table below. Support contact with the provider can be digital in the main but there must be a human contact method available in the event of an internet or connectivity issue. Where phone contact is used, the phone must be answered by a support or customer service contact within 90 seconds. Automated call answering and call queuing, when used, are assumed not to stop the timer.

Mondays	8am to 6pm
Tuesdays	8am to 9pm
Wednesdays	8am to 6pm
Thursdays	8am to 6pm
Fridays	8am to 6pm
Saturdays	9am to 3pm
Sundays & bank holidays	No cover required

- **Remote Access & VPN:** Secure, encrypted remote access shall be provided to enable staff to safely access council servers and files while working from home.
- **Remote support:** It is highly desirable that the provider can remotely access Council-provided devices to diagnose and support issue resolutions. The proposer shall explain how this may be achieved, how security will be controlled and the likely limitations of support this may deliver.

- **Response Times:**

Times in the following table are in hours within a business day, 09:00-17:00. It is assumed that a Ticket number or identification number shall be provided immediately upon completion of reporting the issue. The times below start on the issuing of the ticket.

Activity	All users impacted	Many users	One user
1 st response	Less than 1 hour	Less than 1 hour	Less than 2 hours
Connectivity resolution	Less than 2 hours	Less than 2 hours	Less than 8 hours
Password change or reset where there is no process for Council staff to make the change			Less than 2 hours
Single application issue resolution	Less than 2 hours	Less than 4 hours	Less than 12 hours
Hardware fault	Less than 8 hours	Less than 8 hours	Less than 24 hours

Issue of support ticket number	Automated, immediately issue is reported
1 st response to support ticket	Within 1 hour
Issues around connectivity, passwords, accessing SharePoint	Within 90 minutes
Other software issues	Within 4 business hours
Other hardware issues	Within 8 business hours

- **Annual design review:** The provider shall describe how they would provide a design review each year to recommend any changes to ensure that the solution remains effective.
- **Training and capability building:** The provider shall deliver paper processes and limited training of key support actions to not less than 4 Council staff so that they can carry out the following tasks as a minimum. The proposed solution shall detail processes that the supplier thinks can be carried out by Council staff to minimise the support required by the supplier.
 - a) User password changes/reset
 - b) Removal of user (staff or Councillor) in the event of leaving service
 - c) Changing user profile or security role
 - d) Configuring any proposed automated actions
 - e) Configuring system timers

5. Statutory Compliance & Public Procurement

- **Social Value Act 2012:** Bidders shall demonstrate how they will support the local community, environment, or economy as part of this tender.
- **Transparency and Reporting:** Regular monthly reports detailing system health, outstanding support tickets, and cybersecurity threats

6. Physical data network in the Looe office

- **Data connectivity between the office and Cloud services:** The proposed solution shall ensure that the best use is made of the two internet connections available to the Council to ensure continuity and data speeds for the services used. It is expected that Full Fibre (FTTP) shall be available within 12 months of the letting of this tender.
- **WiFi and physical connections:** The proposed solution shall recommend how best devices shall connect to the network to meet reliability and security requirements. Connectivity is required throughout the building over the two floors.
- **Access to the network:** There are four classes of devices and users that shall be considered: Council-provided devices, Staff BYOD, Councillor devices, and General Public devices. The proposed solution shall ensure that internet and Council data connectivity is available to these classes, meeting the security requirements stated in this tender. It is desirable that the WiFi access SSID names for different device classes have names that make it clear to users which they are connected to. An example of access is provided in the table below;

Device class	Internet access	Councillor data	Council Staff data
Council	Yes	Yes	Yes
Staff BYOD	Yes	No	No
Councillor	Yes	Yes	No
Public	Yes	No	No

Elected councillors

It shall be assumed that Councillors shall desire to use their own devices. This may include Windows, Apple or Android devices.

1. Device Provisioning and Management

- **Tiered Access Profiles:** The proposed solution shall define separate Microsoft 365 profiles for staff versus councillors to restrict sensitive administrative data.
- **Mobile Device Management (MDM):** The solution shall ensure that the Council can remove all Council data from a Councillor-owned device. Where this is not possible, Councillors shall be provided with a secure method of accessing Council data that does not permit the storage of the data.
- **Bring Your Own Device (BYOD) Sandbox:** It is expected that the proposed solution may implement Microsoft Purview or App Protection Policies to containerise council data on personal devices. The tenderer is permitted to propose any solution that meets the needs.
- **Data Leakage Prevention (DLP):** The solution shall ensure that the Council can configure or define rules blocking councillors from copying, printing, or forwarding council emails to personal accounts.

2. Authentication and Identity Security

- **Conditional Access Policies:** The proposed solution shall ensure that the Council can define or implement rules restricting access to personal devices unless they pass specific security health checks.
- **Phishing-Resistant MFA:** The solution shall propose a form of compulsory Multi-Factor Authentication tailored for non-technical users on their personal smartphones and other devices.
- **Single Sign-On (SSO):** The solution proposed shall ensure that there is a unified login system allowing councillors to access all council-permitted portals with one secure credential.

3. Governance and Legal Compliance

- **Offboarding Protocols:** The solution shall propose a manual or automated procedure to instantly revoke data access when a councillor's term ends or they resign.
- **Dedicated Security Training:** It is highly desirable that the supplier shall deliver short, targeted cybersecurity briefings tailored specifically for elected members. These briefings shall be provided within three months of the delivery of the new solution and in the first month following any election of a Councillor or Councillors.

4. Data Segregation Strategy for Councillors

The proposed solution shall restrict councillors to a limited subset of data as required. The proposed solution is expected to review the existing SharePoint data architecture and propose, implement and manage a Hub-and-Spoke SharePoint Architecture. The following architecture is anticipated but the Tenderer is free to propose any similar structure.

- **Staff (Restricted):** The 12 core staff operate in a private, encrypted SharePoint hub containing finance, HR, planning applications, and operations. Councillors are blocked from this hub by default.
- **The Councillor Portal (Accessible):** A separate, simplified SharePoint site acting as a "Councillor Portal". This contains only public agendas, minutes, approved policies, and specific committee folders.
- **Read-Only Enforcement:** It is expected that the solution shall implement a change to the MS-365 licences to ensure that future licenses restrict standard councillors to viewing these documents natively within a web browser or the secure mobile app. This satisfies security needs by preventing them from syncing the council folders to their personal hard drives.

Key dates and Project timeline

Request for tender issued: 31st July 2026

Last date for clarification: 10th August 2026

Tender closing date: 31st August 2026

Tender evaluations commence: 2nd September 2026

Contract awarded: 30th September 2026