REQUEST FOR PROPOSALS

LIMITED-VOLUME STAFF DEVICE SUPPORT & ENDPOINT SECURITY

WORKING DRAFT — Procurement dates, service targets, and contract terms require Logos approval.

RFP detail	Information
Issuing organization	Logos Public Charter School • Medford, Oregon
Issue date	October 29th, 2026
Questions deadline	November 20th, 2026
Proposal deadline	November 27th, 2026
Anticipated service start	January 1st, 2027
Submission contact	accounting@logoscharter.com
Initial term	Up to 12 months; renewal only by written agreement

1. Purpose and award structure

Logos Public Charter School seeks proposals for limited-volume staff device support and ongoing endpoint security administration. This is a standalone procurement. Logos is separately soliciting advanced network administration and infrastructure support and may award that work to another company. The selected provider is not expected to function as a fully outsourced IT department or full-service help desk.

Logos personnel resolve most routine technology questions and perform initial troubleshooting before escalating requests. The selected provider will focus primarily on maintaining appropriate staff-device security controls and will provide occasional escalated technical assistance. The provider must cooperate with Logos staff, the separately selected Network Infrastructure Provider, and Medford School District (MSD) when responsibilities intersect.

2. Operating environment

- Approximately 100 employees with staff laptops; approximately 600 student Chromebooks. Many routine issues are resolved internally before a service ticket is opened.
- Two physical sites with a wireless air bridge connecting the primary and secondary buildings.
- Internet is supplied and managed by Medford School District; Logos' selected vendor does not independently control the upstream connection.
- Recently refreshed UniFi networking equipment; Logos intends to retain its equipment and purchase hardware independently when desired.
- Approximately 100 surveillance cameras; existing UniFi Protect NVR surveillance system.
- MSD manages the telephone service, while phone connectivity depends on switches supported by Logos' IT provider.
- Google Workspace is used for email and documents; Logos does not operate a conventional Active Directory environment.
- Technically capable school employees may provide on-site observation, basic diagnostics, and hands-on coordination with remote network engineers.

Additional sensitive system details may be provided to shortlisted bidders as appropriate. State any assumptions or discovery work needed for accurate pricing.

3. Mandatory requirements

- Hardware independence: Services may not be conditioned on purchasing or leasing hardware through the provider. Provider must support compatible existing equipment and equipment obtained from third parties, subject to clearly disclosed, reasonable technical or manufacturer-support limitations.
- Ownership and access: Logos retains ownership of school-purchased hardware, configurations, credentials, licenses purchased in its name, and school data. Provider shall not withhold administrative access or documentation because Logos changes vendors.
- No forced replacement of recently purchased equipment as a condition of award. Recommended replacements may be offered separately with supporting reasons and optional pricing.
- Initial contract may not exceed 12 months. Renewal or a longer later term requires a new written agreement. Proposed terms must include termination for material or repeated service-level failures with a reasonable opportunity to cure, and transition assistance.
- Provide all recurring fees, hourly rates, travel charges, minimums, emergency premiums, software/license charges, project exclusions, price-increase rules, and offboarding charges. No undisclosed charges.
- Provider must disclose use of subcontractors, including local dispatch partners, and remain responsible for their performance, confidentiality, and applicable school access requirements.
- Maintain appropriate security, confidentiality, least-privilege access, and personnel screening suitable for a K–12 environment. All vendor employees and subcontractors who will be sent on-site to Logos facilities must successfully complete a background check before performing on-site work. Disclose cybersecurity incident response and data handling practices.
- Coordinate promptly and in good faith with the separately contracted technology provider and Medford School District (MSD), where applicable. Share relevant diagnostic findings, identify responsible systems, and participate in joint troubleshooting without unreasonable barriers or blame-shifting. Each provider remains accountable for its own scope and commitments.

4. Scope of services

The Staff Device Support Provider is responsible primarily for staff-device security and limited escalated endpoint support. Logos remains the first line of support for ordinary staff requests. The Network Infrastructure Provider, procured separately, is responsible for UniFi networking, wireless bridges, switches, access points, cameras, and the UniFi Protect NVR.

4.1 Scope

- Establish, verify, maintain, and periodically review appropriate security protections for staff laptops, including endpoint protection, secure configurations, operating-system updates, account/access controls, and response to lost or potentially compromised devices. Identify the ongoing tasks and review frequency included in the proposal.
- Provide escalated diagnosis of staff laptop hardware, software, and peripheral issues only when Logos personnel cannot resolve them internally. Coordinate repair or replacement when appropriate; identify what work is performed directly and what requires a manufacturer or third party.
- Provide occasional remote support or scheduled on-site assistance as necessary. Routine weekly on-site visits, dedicated on-site staffing, and a full-service staff help desk are not requested.

- Advise Logos on practical endpoint security improvements and incident escalation. Clearly distinguish essential controls from optional software or services and explain how recommendations complement Google Workspace and existing school/district systems.
- Refer suspected network infrastructure faults to the separately contracted Network Infrastructure Provider and cooperate with diagnosis when staff devices are affected. This contractor is not responsible for installing or maintaining network infrastructure.
- Student Chromebook repairs and routine Chromebook help-desk services are outside the core scope. Any requested assistance with Chromebook setup or triage must be separately identified and authorized.

4.2 Service delivery and staffing

Expected workload: Logos anticipates fewer than five hours per week on average for routine escalated support and ongoing endpoint security administration under normal conditions. This is a planning estimate, not a guaranteed minimum or maximum. Initial implementation, major security incidents, and separately authorized projects may require additional time. Describe how support is requested, normal availability, remote versus occasional on-site service, personnel and backup coverage, and any minimum charges. Logos prefers a flexible hourly, modest-retainer, or hybrid arrangement rather than mandatory comprehensive per-user managed services.

4.3 Deliverables

- Ticket or work-order record showing request, work completed, time spent, and status.
- Monthly concise summary of security maintenance performed, escalated issues, unresolved risks, and hours or fees billed; identify any action Logos must take.
- Basic staff device inventory, configuration, security-control, and service notes for changes performed.
- Coordination with network infrastructure provider engineers and MSD where staff device issues intersect with network or district-managed services.

5. Division of responsibility and joint incident handling

Responsibility	This contractor	Other separately awarded contractor
Staff laptops, peripherals, OS updates, endpoint protection	Primary	Coordinate / refer
UniFi network, bridge, switches, access points, network security	Coordinate / refer	Primary
Cameras, UniFi Protect NVR, physical network equipment work	Coordinate / refer	Primary
Upstream internet and telephone service	MSD-managed; coordinate as needed	MSD-managed; coordinate as needed
Unclear fault affecting both devices and network	Prompt joint diagnosis and documented handoff	Prompt joint diagnosis and documented handoff

When the cause is unclear, neither provider may close or decline a ticket solely because the issue may belong to the other scope. The receiving provider must document initial findings, notify the appropriate party, and support a coordinated handoff. No contractor is required to perform out-of-scope project work without authorization.

6. Service levels, escalation, and reporting

The RFP separates acknowledgment, qualified investigation, restoration, and permanent resolution. A ticket is not actively investigated merely because an automated reply or account manager acknowledges it. Priority examples below relate to staff endpoints and endpoint security; network outages and wireless bridge failures are the Network Infrastructure Provider's responsibility.

Priority	Example	Meaningful response	Qualified troubleshooting begins	Restoration target / updates
P1 Critical	Confirmed staff-device compromise, ransomware, or serious endpoint security incident	15 minutes	30 minutes	Restore as soon as feasible; updates every 30 minutes
P2 High	Significant endpoint security exposure or multiple staff devices unusable	1 business hour	2 business hours	Target workaround/restoration within 1 business day; updates every 2 business hours
P3 Normal	Escalated laptop/software issue affecting one or a few staff members	4 business hours	1 business day	Target resolution plan within 2 business days; daily updates while active
P4 Routine	Routine device setup, planned maintenance, or minor peripheral request	1 business day	3 business days or scheduled date	Agreed completion date; updates on milestone changes

Definitions: Response = a human acknowledgment that confirms priority, ownership, and next step. Troubleshooting start = qualified technician actively diagnosing. Restoration = core service available again, including an accepted workaround. Resolution = underlying issue corrected and confirmed with Logos. Report all four timestamps separately.

For P1/P2 endpoint incidents, bidders must state coverage hours, after-hours contact procedures, and whether proposed targets use clock time or business time. Restoration and resolution may depend on manufacturers, replacement equipment, or other providers; these dependencies do not excuse timely investigation, updates, and coordination. Bidders may propose clearly identified adjustments to the draft targets.

Proposed accountability: monthly service-level scorecard; repeated material failures trigger a written corrective-action plan; continued failures after cure allow termination without early-termination penalties. Bidders must describe service credits, remedies, and exclusions they propose. Final contract definitions and thresholds are subject to negotiation.

7. Security and software pricing

Logos is seeking effective, appropriately scaled endpoint security management, not an automatically bundled full-service managed IT stack. State the specific protections you will configure, maintain,

monitor, and periodically review. Identify which services are included in the base price and which require separate fees.

- Describe staff endpoint security, MFA/account access coordination, EDR/antivirus, operating-system patching, device configuration, lost-device response, and incident escalation.
- List each proposed security/management product with function, licenses, covered devices, recurring cost, implementation, ownership, and transfer/cancellation terms.
- Identify which products are required for your service model and which are optional, including relevant interaction with Google Workspace and existing school services.
- Describe transfer or removal of endpoint agents, accounts, and tools upon termination.

8. Required proposal format and questions

Use the checklist below as your response outline. Concise answers, short tables, and bullets are encouraged. Explain your actual approach and proposed personnel rather than submitting lengthy generic marketing material. Price for a low-volume, security-focused engagement with Logos providing first-line support.

#	Required response	Include in your answer
01	Support model	Explain how Logos escalates issues after internal triage, your hours of coverage, and how you handle a low volume of tickets.
02	Assigned personnel and backup	Identify the primary endpoint-security/support contact, qualified backup, and escalation contact; explain how coverage works without dedicated on-site staffing.
03	Service-level commitments	Respond to Section 6: human acknowledgment, qualified troubleshooting start, restoration, progress updates, and resolution reporting.
04	On-site service	Explain when occasional on-site visits are needed, scheduling/dispatch arrangements, and minimums or travel fees. No recurring on-site presence is anticipated.
05	Scope and experience	Describe experience providing endpoint security and limited escalated support for an organization of comparable size.
06A	Endpoint security approach	List specific endpoint controls, configuration and review frequency, patching, incident response, products required versus optional, and work included in your fees.
06	Security and background checks	Describe controls within your scope, handling of school data, account access, and completed

		background checks for all on-site staff/subcontractors.
07	Vendor independence	Confirm hardware-purchase independence, continued use of compatible school-owned equipment, school-held access, and transfer at exit.
08	Coordination with other provider and MSD	Describe handoff procedures, incident coordination, and how you will prevent support gaps when causes are initially uncertain.
09	Pricing	Price an expected workload of fewer than five hours per week; provide hourly, retainer, or hybrid options where available. Itemize licensing, onboarding, on-site fees, minimums, and extras.
10	Onboarding and offboarding	Provide a transition plan, documentation approach, and exit process.
11	Business references	Provide 2–3 business references from organizations of similar size and/or structure, with contacts and services provided.
12	Contract exceptions	Confirm a term of no more than 12 months and performance-based termination; list requested exceptions.

9. Standardized pricing response

Cost component	Proposed amount / terms
Optional small retainer / base monthly or annual fee	[Bidder completes]
Included security administration and support hours (if any)	[Bidder completes]
Additional remote hourly rate	[Bidder completes]
Additional on-site hourly rate / minimum	[Bidder completes]
After-hours emergency rate	[Bidder completes]
Travel / dispatch charges	[Bidder completes]
Onboarding / discovery fee	[Bidder completes]
Required software / licenses	[Bidder completes]
Optional software / licenses	[Bidder completes]
Project work / exclusions	[Bidder completes]
Transition / offboarding fees	[Bidder completes]
Estimated year-one total	[Bidder completes]

Provide a realistic first-year total for an engagement averaging fewer than five hours per week of routine support and ongoing security administration, separating fixed fees, variable labor, security licensing, implementation, and optional services. State assumptions and identify how costs change if

usage differs. Hourly, small-retainer, and hybrid proposals are welcome; comprehensive per-user plans are not preferred unless clearly justified.

10. Evaluation methodology

Logos will screen mandatory conditions before scoring. The school may request written clarification and verify qualifications and service quality through references. No technical interview or live exercise is required.

Evaluation criterion	Points
Endpoint security expertise and practical controls	30
Low-volume service model and staffing coverage	20
Endpoint incident response and escalation	15
Clear coordination and scope boundaries	10
Transparent, right-sized cost and value	20
Comparable references and transition readiness	5
TOTAL	**100**

Reviewer guide: 0 = absent; 1 = weak or unsupported; 3 = credible but incomplete; 5 = specific, well evidenced, and supported by personnel, references, or enforceable commitments. Scale ratings to the points shown.

11. Proposed contract principles

- Initial term no longer than 12 months; no automatic multi-year commitment. Extensions and later 2–3-year agreements only by mutual written agreement.
- Define severity levels, clocks, reporting, escalation, and material/repeated failures in the final service-level agreement.
- Termination for cause, including repeated service-level failures after notice and cure; consider a separate termination-for-convenience right with a defined notice period.
- School ownership/control of purchased assets, school data, network configurations, administrative credentials, and transferable school-held licenses.
- Reasonable documented exit assistance, predictable fees, and timely credential/documentation transfer; no withholding of access or forced equipment buyout.
- Written approval before billable projects or changes outside scope; clear change-order process and restrictions on unilateral price increases.
- Clear division of responsibility where MSD, staff device support provider, and network infrastructure provider intersect.

12. Submission and procurement administration

Submit one PDF proposal for this standalone RFP to accounting@logoscharter.com **by Friday, November 27th, 2026**. Questions should be sent to accounting@logoscharter.com **by Friday, November 20th, 2026**. Logos may issue written clarifications to all participating bidders, request written clarifications, check references, negotiate terms, reject proposals, or award this scope separately from the complementary technology services RFP as permitted by applicable procurement rules and school policy. Final dates and procedures must be checked against Logos' governing procurement requirements before publication. Logos reserves the right to disqualify submissions

where there is clear evidence of undisclosed or inappropriate AI-generated questions or answers, particularly where AI is used to misrepresent qualifications, personnel, experience, or technical understanding. Any permitted AI assistance must be reviewed and verified by the bidder; bidders remain responsible for the accuracy and originality of their responses.

For avoidance of doubt, vendors responding to both technology RFPs must submit separate scope-specific proposals and pricing; Logos may select different firms for each.