RAYMORE-PECULIAR SCHOOL DISTRICT

21005 S. School Road, PO Box 789, Peculiar, MO 64078
Phone: 816-892-1300 · Fax: 816-892-1380
www.raypec.org

REQUEST FOR PROPOSAL: RFP Internet Content Filter with Student Safety Monitoring and Classroom Management

Raymore-Peculiar School District is soliciting competitive sealed proposals from IT solutions providers for an Internet Content Filter with Student Safety Monitoring and Classroom Management complying with all terms and conditions described in this document. **Proposals will be accepted by 2:00 p.m. central time, March 15, 2024.** Proposals received after this time will not be accepted.

Mark all documents **RFP Internet Content Filter with Student Safety Monitoring and Classroom Management**. Mail or deliver all proposals and accessory documents to:

Raymore-Peculiar School District
Attn: Pam Steele
Superintendent's Office
21005 S. School Road
Peculiar MO 64078

Proposals must be manually signed on this Raymore-Peculiar School District Form in the space provided below.

Please submit **two paper sets** of your proposal and **one PDF document via thumb drive**. Mark the signed copy as "Original."

Raymore-Peculiar School District reserves the right to accept or reject proposals and to award a contract in the district's best interests.

I have read the terms and conditions of this RFP and submit for consideration the attached proposal and exhibits, if any.

The fees and costs in this proposal have been arrived at independently and have yet to be divulged, discussed, or compared with other Vendors.

I acknowledge that no conflict of interest is defined in Regulation 4840 here.

By signing below, the Proposer agrees to the district policies for requesting proposals.

_____ Company Name	_____ Contact Name
_____ Company Address	_____ Contact Phone Number
_____ Company Telephone Number	_____ Authorized Name and Title
_____ Company Fax Number	_____ Authorized Signature and Title

1. Objective

The purpose of this document is to request Vendor proposals and pricing for commercial off-the-shelf Internet Content Filter with Student Safety Monitoring and Classroom Management solutions, tailored to integrate seamlessly into the Raymore-Peculiar School District network environment. Desired features specific to the district's needs are detailed in the specifications section below. Vendors are expected to address each section applicable to their offerings, providing comprehensive explanations of how their product meets the specifications and aligns with the proposed solution. Raymore-Peculiar School District reserves the right to award the contract to a single Vendor capable of meeting all requirements or to multiple Vendors for different sections of the specifications.

Raymore-Peculiar School District may decide to pursue a demonstration of any one or multiple Vendor products before making a final determination. The demonstration may consist of any Vendor who can provide a solution for the entire requirements section or multiple Vendors for individual sections of this RFP.

2. Terms

The **Raymore-Peculiar School District** or "**The District**" or "**RPSD**" shall refer to the party seeking submissions for solutions aligned with the specifications in the sections below.

A **Submitting Vendor** or "**Vendor**" shall refer to any individual or entity submitting proposals in response to the RFP.

The **System(s)** shall refer to all hardware and software to be proposed by the Vendor.

The **Internet Content Filter** or "**ICF**" shall refer to the system proposed by the Vendor to the District.

The **Student Safety Monitoring** or "**SSM**" shall refer to the system proposed by the Vendor to the District.

The **Classroom Management** or "**CLM**" shall refer to the system proposed by the Vendor to the District.

Active Directory or "**AD**"

Google Workspace or "**GW**"

3. Scope

The scope of this document is to delineate the specifications for an Internet Content Filter with Student Safety Monitoring and Classroom Management system tailored to meet the needs of RPSD. Vendors are invited to submit a single technical response covering either the entire scope of requirements or specific sections based on their solution capabilities. The response should be structured in paragraph form, addressing each section of the RFP.

The District is seeking a modern and innovative system for Internet Content Filtering with Student Safety Monitoring and Classroom Management that can efficiently identify and mitigate online threats in real time. The solution should demonstrate adaptability, customization, reliability, and low impact to the overall end-user experience in a Globally Connected Internet while also maintaining an understandable and logical management interface.

This System shall meet or exceed the requirements listed in the Specifications section to serve the RPSD hardware environment and end users described in the Background section.

4. Background

The District serves approximately 6500 Kindergarten through 12th Grade Students in a one-to-one device environment featuring the following;

- PK-1 use iPads
- 2-12 use Chromebooks
- 2-12 have access to Windows PC and iMac Computer Labs
- Student access to various Internet of Things devices such as 3D Printers.
- Student Medical Devices such as but not limited to Android Phones, blood glucose meters, or heart monitors.

The District also serves approximately 1100 full or part-time staff members featuring the following;

- Teachers with one-to-one Macbooks and access to Windows PCs.
- Administrative and support staff members with access to Macbooks or Windows PCs.
- Staff members with access to BYOD (Bring Your Own Device) network.
- Network Infrastructure including Windows and Linux servers, appliances, and switches.

All one-to-one devices for both staff and students are available for at-home use. The District also maintains two distinct connections to the Internet for redundancy purposes, each with a dedicated firewall.

The **current ICF** solution utilized by the District is **iBoss**.

The **current SSM** solution utilized by the District is **Gaggle**.

The **current CLM** solution utilized by the District includes **Lenovo LanSchool** and **Hapara**.

Questions for additional information should be communicated to Ryan Gooding at 816-892-1333 or ryan.gooding@raypec.org.

5. Specifications

The System requirements are listed in the sections below. Where the Vendor system is not applicable or compliant, the Vendor response shall specify such lack of compliance or a suitable alternative to accomplish the same goal. Vendors may respond to all the requirements, or to only specific major subsections. **Vendors are also encouraged to provide details of features not indicated in the specifications that may add value to the District.**

5.1 *Internet Content Filtering* (ICF)

- Filters web content based on predefined categories, keywords, or custom rules to prevent access to inappropriate or harmful websites.
- Ability to distinguish between and block traffic from Proxy and AI resources with measures for managing allowed websites.
- Manages access to web-based applications and services, allowing administrators to block or restrict usage of specific applications to maintain productivity and security.
- Decryption and inspection of SSL/TLS encrypted traffic to identify and block threats hidden within encrypted connections, providing comprehensive content management.
- Utilizes advanced threat detection technologies to identify and block malware, ransomware, and other malicious or inappropriate content before it reaches end-users devices.

- Automatic and frequently updated website categories, keywords, web-based applications and services, and known or emerging threats to ICF policy circumvention.
- Controls and optimizes network bandwidth usage by prioritizing traffic, limiting bandwidth-intensive applications, and preventing bandwidth abuse to ensure efficient network performance.
- Provides real-time visibility into web usage and security events through comprehensive reporting and analytics, enabling administrators to monitor network activity and identify potential threats or policy violations.
- Offers granular policy configuration options, allowing administrators to define specific rules and exceptions based on user roles, AD or Google groups, devices, IP address subnets, age, grade, class, or school to tailor security policies to their organization's needs.
- Schedule-based policy configuration that sets specific rules and regulations for in-school, after-school, and nighttime activities, ensuring coverage of all operational periods.
- Supports various methods of user authentication, including Active Directory integration, Google single sign-on (SSO), and multi-factor authentication (MFA), to ensure secure access to network resources and apply appropriate policies based on user identity.
- Integration with the Student Information System Focus School Solutions.
- Integration with ClassLink for rostering of student classes and schedules.
- Analytics reporting to track usage and engagement of school-related applications and resources on any device and across any browser.
- Manages BYOD (Bring Your Own Device) Wi-Fi networks and access, providing secure internet access for visitors while protecting the organization's network from potential threats or misuse.
- Helps organizations achieve regulatory compliance by enforcing policies related to data protection, privacy, and acceptable use, and generating compliance reports for auditing purposes to include CIPA, COPPA, and FERPA compliance specifically.
- Integrates with threat intelligence feeds and databases to enhance threat detection capabilities and provide real-time protection against emerging threats and zero-day vulnerabilities.
- Scalability to accommodate the growing needs of the Raymore-Peculiar School District and ensures high availability through redundant architecture and failover mechanisms.
- Centralized management console for System administrators to configure, monitor, and manage all aspects of the content filtering solution from a single interface, simplifying administration and maintenance tasks.
- Hierarchical management policy to empower user control in the classroom environment while pradhering to administrator mandated policies.
- Cloud based System with no or minimal on premise hardware or software.
- Equitable functionality for all devices across all platforms in use by the District including Chromebooks, Windows PCs, iOS devices, Mac OS devices, Windows Servers, Linux Servers, network appliances, and IOT (Internet of Things) devices.
- Maintain all ICF functionality for student devices during at-home use.
- Automated report delivery showing traffic patterns, detections, and other custom reports.
- Integration with YouTube video access management with logging for approvals and simple reporting.
- Support Mobile Device Management deployment solutions including Mosyle, PDQ Deploy, and Google Workspace.
- Vendor System support services including phone, chat, and email contact information.
- Vendor System training for all levels of access to the System.

- The District shall maintain full and exclusive management access to every component of the Solution whereby the only exclusions are absolutely necessary support access by the Vendor logged and reported to RPSD.

5.2 *Student Safety Monitoring* (SSM)

- Offers parents and guardians the ability to view their child's digital learning activities and progress, fostering a closer connection between home and school. Each feature of the system is under the district's complete control, allowing them to activate or deactivate it as needed.
- Monitor students' online activity, including emails, attachments, files, documents, and messages, for signs of inappropriate content, self-harm, cyberbullying, violence, or other concerning behavior across platforms.
- Utilizes artificial intelligence and machine learning algorithms to analyze content and identify potential safety risks, enabling timely intervention by school officials.
- Provides continuous monitoring of students' digital communications and interactions, ensuring that safety concerns are addressed promptly, even outside of school hours.
- Allows district administrators to customize alerting criteria based on their specific safety policies and concerns, ensuring that relevant incidents are flagged for review.
- Employs a team of trained safety experts to review flagged content, assess the severity of the situation, and take appropriate action, such as notifying school officials or law enforcement if necessary.
- Has the ability to notify parents or guardians of students involved in safety-related incidents, providing transparency and fostering collaboration between schools and families in addressing student safety concerns.
- Generates reports and documentation to demonstrate compliance with legal requirements and regulations related to student safety, such as the Children's Internet Protection Act (CIPA) and state-specific laws.
- Integrates with popular education platforms and communication tools used by schools, such as Google Workspace (formerly G Suite), Microsoft 365, and Canvas, to ensure comprehensive coverage of students' digital activities.
- Implements robust security measures and data protection protocols to safeguard student information and ensure compliance with privacy regulations, such as the Family Educational Rights and Privacy Act (FERPA).
- Offers resources and training materials for educators, students, and parents on digital citizenship, online safety, and responsible technology use, promoting a culture of digital wellness within the school community.
- Specifically identifies and flags instances of cyberbullying, harassment, or intimidation among students, helping schools address these harmful behaviors and promote a positive school climate.
- Recognizes indicators of suicidal ideation or self-harm in students' digital communications and alerts school officials to provide appropriate support and intervention.
- Provides students with a confidential mechanism to report safety concerns or incidents they witness or experience online, encouraging proactive reporting and intervention.
- Extends monitoring and safety features across various digital platforms and communication channels commonly used by students, including email, social media, online forums, and messaging apps.
- Facilitates coordination between school officials, law enforcement, and other relevant stakeholders in responding to critical incidents or emergencies involving student safety issues.

5.3 *Classroom Management* “CLM”

- Provides teachers with a centralized dashboard to monitor student activity and engagement across various digital tools and platforms.
- Allows teachers to create customized digital workspaces for each class, facilitating organization and collaboration among students.
- Enables teachers to view real-time student activity within digital applications, including websites visited and documents accessed.
- Allows teachers to monitor students' screens during class to ensure they are on task and following instructions.
- Provides teachers with the ability to remotely lock students' screens or guide them to specific websites or applications.
- Facilitates the sharing of resources, assignments, and feedback between teachers and students.
- Integrates collaborative tools such as Google Workspace (formerly G Suite) to promote teamwork and communication among students.
- Provides insights into student engagement, progress, and performance through analytics and reporting features, helping teachers make informed instructional decisions.
- Integrates with Canvas, enhancing existing digital learning environments.
- Ensures student data privacy and compliance with relevant regulations through robust security measures and data protection protocols.

5.4 *Deployment Architecture*

Detail any software or hardware that must be installed and changes to servers, devices, or the District network devices required for System deployment. Details should include the specifications of the software agents or hardware that is to be deployed including update frequency and strategy.

5.4.1 Integration Requirements

The product should fulfill the following integration requirements

- The agents should be compatible with popular operating systems such as MacOS, IOS, popular Windows distributions (such as Server 2012, 2016, and 2019, 2022), along with workstation variants (10 and 11), and recent versions of Chrome OS.
- User authentication, including Active Directory integration, Google single sign-on (SSO), and multi-factor authentication (MFA), to ensure secure access to network resources and apply appropriate policies based on user identity.
- Automated Focus Student Information System for student account identification, class schedules, and teacher associations.
- Automated On-Premise AD synchronization for staff account identification and group association.
- Automated direct CSV Import for staff account identification and group association.
- Other requirements listed in pertinent System sections above.

5.4.2 Remote Management

The System shall be manageable remotely via an encrypted channel. Describe the method of remote support and the total number of users that may be supported simultaneously.

5.4.3 Database Maintenance

If the System utilizes a database, it shall use a self-maintaining database or maintenance procedures shall be exhaustively defined. Predefined scripts or controls shall be in place to manage archive, retention, and purging. Vendors must also describe database security capabilities including masking, encryption, monitoring, etc.

5.5 *Authentication and Role-Based Management*

The goal of this requirement is twofold. The first goal is to provide a centrally managed point of authentication for the product management console. The second is to provide a means for a clear separation of duties.

5.5.1 Authentication Protocols

The product shall allow role-based access via modern authentication protocols. Please list which authentication methods the tool interfaces with (LDAP, Google, etc.).

5.5.2 Multi-Factor Authentication

The product shall allow integration with Multi-Factor Authentication systems for access control or another comparable solution.

5.6 *Logging Mechanism*

5.6.1 Log Retention

The System shall be capable of providing searchable logs capable of automatic rotation. For the purposes of Vendor proposals, the System shall be sized to maintain logs on the device for a minimum of 90 days and shall be capable of automatically exporting logs for archival storage. The number of days logs are retained shall be configurable, and Vendor responses shall describe the configuration mechanism.

5.6.2 Auditing Records

The Vendor will provide, at a minimum, reportable audit records for system administration activities that will include login/logoff, configuration changes, reporting, role changes, system start-up and shutdowns, and other administrator activities.

5.7 *Current Production Release*

Software/hardware and all software/hardware features proposed must be commercially available, current general deployment, and production versions at the time the response is written.

5.7.1 OS (Operating System)

The Vendor shall define what operating system, including hardware platform, their product employs and what version and patch level is current.

5.7.2 Patch Maintenance / Software Release Cycle

The Vendor shall define how patches are deployed to their system, whether automatically or manually, and typical new software release cycles. Additionally, Vendor responses shall include software and base system ICF, SSM, and CLM features and capabilities. For example, if the proposed solution is Windows or Linux based the timeline between patch release and Vendor support of patch release shall be detailed with examples.

5.7.3 Open-Source Components

Please list any relevant open-source components or dependencies of this application. Specifically how will the Vendor resolve issues in open-source components if the open-source component is abandoned by its maintainers or found to have vulnerabilities?

5.8 *Raymore-Peculiar School District Infrastructure Components*

Support for current **District** infrastructure components shall be included in the Vendor's current commercial product release. **RPSD**'s infrastructure is composed of Cisco, Aruba, HP, Windows, Chrome, MacOS, iOS, and Linux devices. In your response, please be clear about which systems, standards, Vendors, etc. your solution is designed to interface with or otherwise integrate with.

5.9 *Hardware / Software Platforms*

The Vendor response shall include a specification and description of all hardware and software components. This specification shall include operating system, network capabilities, and other key components for the solution.

5.9.1 Detailed Architecture

Vendors shall include a detailed illustration of the System to meet or exceed District requirements. The Vendor shall also include a redacted report providing the capabilities of the product.

5.9.2 Detailed Hardware/Software Specification

Vendor proposals shall include a detailed hardware specification. The detailed hardware or software specification shall include specifications for CPU, RAM, fixed internal and external disk arrays, network connection support, network bandwidth available, and other pertinent hardware specifications. The proposed System shall operate with full functionality with no or minimal impact on end-user experience under all circumstances while meeting all applicable requirements.

5.10 *Licensing*

The Vendor response shall include a detailed explanation of the licensing model. If you offer multiple licensing models, please provide subscription and perpetual capital licensing options.

5.11 *Performance*

5.11.1 Skill Requirement

The Vendor response shall include the level of expertise required by a support personnel.

5.11.2 Available training

Vendor response shall detail available formalized training for the System including any onboarding processes.

5.12 *Support Policies*

The response shall provide an overview of support policies and include a vendor-recommended support and maintenance contract in the response for one year with an optional two-year extension. The level of service provided and the location of support centers shall be clearly defined. Support service channels should also be clearly defined such as Chat, Phone, or Email with an associated response time. Vendor responses must include a support operations schedule, locations of support centers, and handoff mechanisms. The Vendor shall describe any support function and levels supported outside of the United States.

5.13 *Statement of Work*

The response shall include a statement of work detailing all phases required to implement a complete production implementation at the District, as defined in the paragraphs above. This statement of work shall include, but may not be limited to, installation, filter preference transition from current ICF, SSM, and CLM, reporting mechanisms, and support procedures. If the statement of work includes items the Vendor believes require Vendor consultation for implementation, this should also be stated. All items and services listed in the statement of work should be included in the final price to the district.

5.14 *Product Background & References*

5.14.1 Release Date

The Vendor shall define the date when the base product became a commercial offering and the current release.

5.14.2 Proof of Concept

The District may elect to perform a limited proof of concept of select Systems if necessary to the selection process.

5.14.2 References

Provide other education customers that you currently serve in the Kansas City or Missouri/Kansas area.

6. Deliverables

The solution in the Vendor's informational proposal shall include all required software, use licenses, software media, and/or updates as required. Additionally, any professional services deemed to be required for successful implementation should also be specified. If the System includes Vendor-specific hardware appliances, these items shall be added to the response. Similarly, if the System does not require Vendor-specific hardware appliances, estimated hardware requirements shall be added to the response.

The Vendor response shall include all software or hardware components required to implement a complete system as outlined in the Requirements section above. Where components are required, but not included or available from the Vendor, please identify those in the response.

7. Submission Requirements

1. Vendors will submit a document describing the corporation and the breadth of its services offerings, as well as the firm's length of experience in field of content filtering, including participation in professional forums and symposiums, as well as professional organizations.
2. The Vendor will include pricing for a turnkey System, encompassing any supplemental hardware or software needed by the District to implement the product effectively. Pricing should encompass options for contracts spanning 1, 3, and 5 years.
3. Vendors are required to provide a technical proposal that addresses all the subsections of section 5. This proposal must include the information requested in the previous sections. Each vendor must fully respond to all items in Section 5 (Specifications) and refer to the appropriate section and subsection numbers in this document. The total length of the proposal should not exceed twenty-five pages.
4. Vendor will submit two paper sets of your proposal and one PDF document via thumb drive. Mark the signed copy as "Original."

5. Information provided to Vendors in reference to this project will be treated as **RPSD confidential and will not be disclosed to third parties without the written consent of the District**.