2026-2027

Data Security & Internet Safety

Annual District Review

Purpose Provide an annual, plain-language review of how Menifee County Schools protects student and staff information, secures district systems, and promotes safe internet use.

Prepared by
Mark Clemons, CIO/DTC
August 2026

Executive summary

Menifee County Schools continues to strengthen security through layered identity, endpoint, network, email, and internet-safety controls. The district is moving toward the Kentucky Connected User Experience System (CUES), powered by RapidIdentity, while expanding multi-factor authentication and modernizing endpoint protection and management.

Current-year focus Complete staff CUES account claiming and federation readiness, finish the transition from Trellix to Microsoft Defender, verify backup and recovery practices, and continue centralized patching and security monitoring.

Report information

School year	2026-2027
Report date	August 2026
Report owner	Mark Clemons, CIO/DTC
Next formal review	Summer 2027, or sooner after a material security change

At-a-glance control status

Status	Security control / activity	Owner / cadence
Implemented	Cloud content filtering, managed district accounts and devices, layered firewall protection, phishing safeguards, and centralized device administration.	Ongoing
In progress	Action1 software deployment, patch management, inventory, and remote support is active on approximately 80% of Windows endpoints, with districtwide completion planned during 2026.	Technology / Target: 2026
In progress	CUES/RapidIdentity account claiming, Microsoft Authenticator enrollment, and federation preparation.	Technology + staff
In progress	Replacement of Trellix with Microsoft Defender and confirmation that Defender is active and current.	Technology
Annual review	Backup recovery testing, incident-response contacts, evidence retention, and shared security responsibilities.	District leadership + departments

1. Protecting student and staff information

Personally identifiable information (PII) is information that can identify or be linked to a specific person. Examples include names, student or employee identifiers, Social Security numbers, addresses, telephone numbers, email addresses, login identifiers, IP addresses, photographs, education records, and combinations of data that can identify an individual.

District safeguards

- Limit access according to job responsibilities and remove access when employment or duties change.
- Use managed accounts and district-controlled devices for district business.
- Apply password, authentication, filtering, and monitoring controls appropriate to the system and user group.
- Review external sharing, group membership, privileged access, and unusual sign-in activity.
- Protect downloaded reports and local files through approved district storage, access controls, and proper disposal practices.
- Use role-based security and privacy training, including CJIS requirements where applicable.

Annual evidence to retain

Status	Security control / activity	Owner / cadence
Annual review	Current acceptable-use, data-security, incident-response, password, and internet-safety policies.	Technology
Annual review	Staff training completion, simulated-phishing or awareness records, and security communications.	Technology
Annual review	Access reviews for administrators, finance, student information, email, and other sensitive systems.	Technology
Annual review	Backup test results, vulnerability/patch reports, endpoint protection status, and incident records.	Technology

2. Identity, access, and CUES modernization

The district is transitioning identity services toward CUES and RapidIdentity. This work is intended to provide a more consistent sign-in experience, improve account lifecycle management, strengthen authentication, and support Kentucky's long-term identity modernization.

2026 implementation activity

- Staff receive a RapidIdentity account-claiming message titled ‘Welcome to Menifee County District’ from noreply@rapididentity.com.
- Microsoft Authenticator is being used as the district's preferred authenticator for staff multi-factor authentication.
- The district is preparing for federation so participating services will rely on the new identity path for authentication.
- RapidIdentity provisioning is being coordinated with Active Directory, Google Workspace, Microsoft 365, and Infinite Campus-related identity processes.
- Account creation, transfers, authorization changes, and terminations are reviewed as part of the account lifecycle.

> **Progress snapshot** As of August 18, 2026, 80 of 194 staff accounts (41%) had completed account claiming. Remaining staff require direct follow-up before federation.

Identity security priorities

- Complete staff account claiming and verify recovery methods before federation.
- Maintain a documented process for personnel who cannot use a personal mobile phone.
- Use least privilege for administrative roles and review membership in privileged or districtwide groups.
- Document where device identities and other identity-dependent records will be retained as legacy Active Directory services change.
- Test new-user provisioning from source data through Microsoft 365 and Google account availability.

3. Endpoint security and device management

District Windows computers, Chromebooks, and Apple devices are managed through platforms appropriate to each device type. Central management helps standardize security settings, software, updates, inventory, and support.

Windows endpoints

- Action1 provides centralized inventory, software deployment, patching, and remote support and is deployed to approximately 80% of district Windows endpoints. The district plans to complete deployment during 2026.
- Microsoft Defender is replacing Trellix as the standard Windows endpoint protection platform.
- Windows 11 Pro is used for newly imaged staff devices, with current operating-system and driver updates.
- GoGuardian software is deployed where required for student-safety and classroom monitoring functions.

Chromebooks and Apple devices

- Chromebooks are enrolled and managed through the district's Google environment, with model age and Auto Update Expiration dates tracked for replacement planning.
- A Chromebook refresh target of 15% of the student fleet is recommended annually, with serviceable retired devices retained as controlled spares.
- Apple devices are managed through Apple School Manager and Mosyle where applicable.
- Only district-authorized accounts should be used to access district-managed devices and services.

Patch and vulnerability management

- Test material updates when practical before wide deployment.
- Prioritize security updates based on severity and exposure.
- Use centralized deployment and reporting to confirm installation.
- Maintain rollback or recovery options when an update causes operational problems.

4. Network, physical security, and internet safety

Internet access is protected through KETS network services, layered firewall controls, filtering, managed wireless infrastructure, and district policy. Controls are reviewed as applications, devices, threats, and instructional needs change.

Current protections

- GoGuardian web filtering for district-managed devices and student accounts.
- Layered firewall and KETS network protections that restrict unauthorized external connections.
- Managed Juniper Mist wireless access points and segmented network services.
- Managed DNS and DHCP services, including KETS/Infoblox components where assigned.
- Review of filtering and internet-activity reports by authorized district and school administrators.
- District-account requirements on managed devices to reduce anonymous or unmanaged access.

Physical access and safety systems

District facilities use centrally managed Verkada electronic access badges and Wisenet video-surveillance systems. Access credentials are monitored and automatically deactivated after extended inactivity; lost, compromised, or former-employee credentials are promptly disabled. Authorized personnel use video surveillance to support facility safety, incident review, and the protection of students, staff, and district property.

Student internet safety

- Age-appropriate filtering and safe-search controls.
- Digital citizenship and responsible-use expectations.
- GoGuardian monitoring, alerting, and classroom-management capabilities where deployed.
- Investigation and escalation of alerts involving self-harm, violence, exploitation, or other student-safety concerns according to district procedures.
- Periodic review of blocked categories, exceptions, and educational access needs.

> **Important distinction** Filtering reduces risk but cannot replace supervision, digital citizenship instruction, staff awareness, or incident reporting.

5. Email, phishing, and account protection

Phishing and credential theft remain significant risks because attackers often target people rather than technology. Menifee County Schools uses technical safeguards together with staff awareness and rapid reporting.

Layered protections

- Microsoft 365 anti-spam and anti-phishing policies, including quarantine for high-confidence phishing.
- External-email identification, Safe Links, Safe Attachments, and data-loss-prevention capabilities where licensed and configured.
- PIXM phishing protection and continued review of available protections.
- Multi-factor authentication through the CUES/RapidIdentity transition.
- Review of unusual sign-ins, location information, repeated failures, and other account-risk indicators.
- Staff reminders to verify unexpected requests and never share passwords or MFA verification codes.

What staff should report immediately

- An unexpected MFA prompt or authentication code request.
- A suspected phishing message, malicious attachment, or credential-entry page.
- A lost or stolen district device or phone used for district authentication.
- Unexpected account activity, password changes, sent messages, or access denials.
- Any suspected exposure of student, employee, financial, health, or criminal-justice information.

6. Backup, recovery, and incident response

Security planning assumes that prevention may fail. The district therefore maintains incident-response procedures and should verify that critical information can be restored from protected backups.

Incident-response readiness

- A School Cyber Attack Response Playbook was prepared for Menifee County Schools in May 2026.
- Response priorities include containment, account protection, evidence preservation, continuity of operations, recovery, and required notifications.
- Technology, district leadership, legal/privacy contacts, KETS/KDE, insurance, law enforcement, and vendors are engaged according to the nature and severity of an incident.
- Unusual activity should be reported immediately rather than investigated independently by end users.

7. Priorities for 2026-2027

Status	Security control / activity	Owner / cadence
In progress	Complete CUES/RapidIdentity staff claiming, federation readiness, and exception handling for users without mobile phones.	Target: Fall 2026
In progress	Finish Trellix removal and verify Microsoft Defender health, updates, exclusions, and reporting across Windows endpoints.	Target: 2026
Annual review	Complete Action1 deployment to remaining Windows endpoints and formalize monthly patch/vulnerability evidence and an exception process for devices that cannot be updated promptly.	Technology / Target: 2026
In progress	Review artificial-intelligence tools and develop district guidance consistent with KDE recommendations, emphasizing approved tools, student and staff data privacy, human review of AI-generated content, academic integrity, transparency, and responsible use. Confidential or personally identifiable information should not be entered into unapproved AI services.	Technology + leadership / 2026-2027
Annual review	Verify backup restoration, alternate-copy protections, and incident-response contacts.	Technology / leadership
Annual review	Continue security awareness through concise Menifee Tech Minute messages when staff action is required.	As needed
Annual review	Maintain the recommended annual Chromebook refresh target of 15% and a working spare pool.	Budget cycle