

Google Workspace Email Security for Schools

Practical district checklist

Use this checklist to review the district's sending inventory, domain authentication, Gmail controls, administrative access, and incident readiness.

1. Know the environment

- ☐ Inventory primary, secondary, alias, student, and campaign domains.
- ☐ Record every SaaS platform, relay, device, and service that sends as a district domain.
- ☐ Document inbound gateways, routes, forwarding, journaling, and archives.
- ☐ Name the business and technical owner for every sender and exception.

2. Authenticate district mail

- ☐ Publish one valid SPF record per sending domain and review recursive lookup depth.
- ☐ Enable DKIM for Google Workspace and every approved third-party sender.
- ☐ Verify delivered messages after gateways or services that may modify content.
- ☐ Collect DMARC aggregate reports and resolve unknown or misaligned sources.
- ☐ Advance DMARC policy gradually only after representative mail is understood.

Test first

Run a domain posture scan at hootshield.com, then verify representative delivered messages before changing enforcement.

3. Review Gmail protections

- ☐ Review protections for unusual, scripted, encrypted, and untrusted attachments.
- ☐ Review shortened-link, external-image, and untrusted-domain protections.
- ☐ Review employee-name, lookalike-domain, and unauthenticated-message defenses.
- ☐ Give every allowlist or bypass a reason, owner, scope, and review date.
- ☐ Test changes with a controlled group where possible.

4. Protect identity and administration

- ☐ Use separate administrator and daily-work accounts.
- ☐ Keep super administrator membership small and reviewed.
- ☐ Require strong, preferably phishing-resistant, multifactor authentication.
- ☐ Review OAuth applications, recovery methods, delegates, and app passwords.
- ☐ Assign owners for suspicious login, forwarding, routing, and delegation alerts.

5. Prepare response

- ☐ Define report, triage, containment, investigation, communication, and recovery roles.
- ☐ Preserve message IDs, timestamps, account events, tokens, rules, and evidence.
- ☐ Rehearse a compromised-account scenario with technology, communications, and finance.
- ☐ Record provider actions and confirm whether each one succeeded.