

Know Your Gaps. Before the Auditor Does.

Five questions that reveal where your Washington district really stands on cybersecurity, student-data protection, and incident response, before your next compliance audit or insurance renewal.

Your compliance audit is coming, and you have to prove controls are in place across cybersecurity, data protection, and incident response. Most districts do not know where they actually stand: the gaps are not obvious until an auditor finds them. Answer these five questions first.

ASK YOUR TEAM THESE 5 QUESTIONS

- 1** Have you formally adopted a cybersecurity framework, and can you show where your district stands against it today?

MAPS TO: NIST CSF 2.0 • CIS Controls • Cyber-Insurance
- 2** Can you name every system that touches student data and prove each vendor contract meets state and federal privacy law?

MAPS TO: FERPA • COPPA • WA SUPER Act (RCW 28A.604)
- 3** Is your content filtering and internet-safety policy current and documented enough to pass a CIPA review and protect E-rate funding?

MAPS TO: CIPA • E-rate
- 4** Do you have a written, tested incident response plan, and do you know your breach-notification deadlines before an incident hits?

MAPS TO: Incident Response • WA Breach Notification (RCW 42.56.590)
- 5** If ransomware struck tomorrow, could you restore from tested backups, with MFA and least-privilege access enforced district-wide?

MAPS TO: Backup & Recovery • Access Control • MFA

100%
EXAM PASS RATE, STAGE 3+

WLS343
CONTRACT • NO RFP

ONE
ROADMAP, NOT MANY
VENDORS

24/7/365
U.S.-BASED SOC

4.95 / 5
CLIENT CSAT

See Where Your District Stands.

30 MINUTES • NO COST • NO RFP

Book a 30-minute call or request your assessment. We will benchmark your district against current K-12 requirements and hand you one clear roadmap, through the WLS343 contract. No RFP, no delays.

EMAIL

support@torchlight.io

WEB

TorchLight.io

24/7 EMERGENCY HOTLINE

833-761-0695

BOOK A MEETING →