



Five Steps to Reducing Cloud Workspace Risk **This Academic Year**

A Guide to Securing Educational Environments



Cyber Resilience for Modern Education

Schools rely on cloud workspaces every day, but protecting data, users, and communications requires more than the platform alone. As we enter the new academic year, having an effective security architecture is essential. XMA, in partnership with Barracuda, provides the complete cyber resilience your organisation needs to maintain learning continuity and keep students safe and secure.



Five Challenges Facing School IT Teams



Data deletion and loss:

Under the cloud shared responsibility model, native environments do not fully protect configuration data, policies, or user assignments from accidental or malicious deletion.



Compliance and accountability:

Safeguarding student data and maintaining learning continuity are paramount.



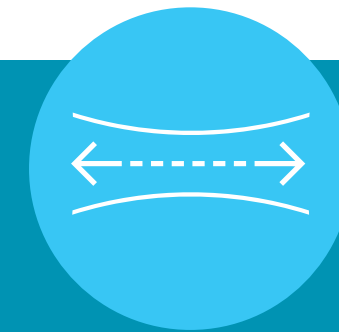
Growing ransomware threats:

Growing ransomware threats: Ransomware incidents continue to rise, with schools being a prime target for cyber criminals.



Phishing and email compromise:

Educational institutions are increasingly targeted by sophisticated phishing campaigns. Email remains the most common entry point for cyber threats into corporate networks.



Limited IT resources:

School IT teams face unique challenges, balancing strict budget pressures and resource constraints.



What Happens When Risks Aren't Addressed

Lost mailbox = Teaching disruption:

Missing curriculum resources and costly downtime can severely impact school operations.

Compromised account = Data exposure:

Missing curriculum resources and costly downtime can severely impact school operations.

Five Steps to Strengthen Cyber Resilience

1

Understand your cloud responsibilities:

Cloud providers manage infrastructure uptime, but ultimate accountability remains with the school.

2

Protect critical data with Barracuda backup and recovery:

Cloud-native Barracuda backup engines ensure complete data sovereignty and fast, reliable recovery.

3

Strengthen email security with Barracuda:

AI-powered threat detection from Barracuda identifies abnormal communication patterns to block sophisticated conversation hijacking before it reaches user inboxes.

4

Create a recovery plan before an incident occurs:

XMA manages the full implementation process, ensuring Barracuda technology works reliably with your broader IT ecosystem without disrupting operational workflows.

5

Improve visibility into threats:

Improve visibility into threats: Identity systems have become prime targets. Implementing Barracuda monitoring tools allows you to track suspicious account changes, such as unauthorised email forwarding.



Start Your Free Trial Today

Enjoy a 14-day Barracuda trial with no commitment.

XMA partners with Barracuda to deliver unified, business-grade cybersecurity platforms. Ready to evaluate your current defence posture risk-free?

Book a free consultation with our Cyber Security expert, Rhys Gansen-Jones:

CLICK HERE TO BOOK YOUR MEETING



0115 846 4000



xma.co.uk



enquiries@xma.co.uk



@xma



@WeareXMA