Nottingham cyber attack highlights why education security is about more than IT

nottinghamworld.com/your-world/nottingham-cyber-attack-highlights-why-education-security-is-about-more-than-it-8672729

Kevin Walker June 11, 2026

Kevin Walker of Black Swan Cyber Security Solutions reviewing incident logs. | Black Swan Cyber Security Solutions

Cyber security specialist says incidents affecting schools, colleges and universities can quickly become issues of safeguarding, learning, communication and public trust.

Recent reports of a cyber attack affecting the University of Nottingham have highlighted how damaging data breaches can be for education providers, students, alumni, staff and families.

The University of Nottingham has confirmed that a cyber criminal group accessed personal data held in its student records system. According to reports, the university has contacted those affected and reported the incident to Action Fraud and the Information Commissioner’s Office.

Kevin Walker, founder of Black Swan Cyber Security Solutions, says the incident is a reminder that cyber security in education is not just a technical concern.

“When people hear ‘cyber attack’, they often picture an IT problem,” said Kevin. “But in education, it can become a safeguarding, continuity and communication problem very quickly.

“If a school, college or university loses access to its systems, or if personal data is accessed, the impact can be felt far beyond the IT department. It can affect student records, safeguarding information, parent and carer contact details, finance, payroll, exams, lessons and public confidence.”

Kevin, who has over 20 years’ experience supporting education IT, says schools, colleges and universities are often dealing with cyber security alongside tight budgets, staffing pressure, compliance demands and the day-to-day work of keeping education running.

“Most education settings are not ignoring cyber security,” he said. “The issue is often capacity. IT teams are stretched. Leaders are under pressure. Systems are complicated. Third-party platforms hold large amounts of data. That is why cyber resilience needs to be treated as part of business continuity, not as something bolted on after the event.”

The latest Government Cyber Security Breaches Survey found that 49% of primary schools, 73% of secondary schools, 88% of further education colleges and 98% of higher education institutions identified a cyber breach or attack in the previous 12 months.

Kevin says education leaders and governors should use recent incidents as a prompt to ask practical questions rather than panic.

These include:

- When did we last test our backups?
- Could we restore our most important systems quickly?
- Is multi-factor authentication in place for key accounts?
- Are Microsoft 365 and email accounts monitored for suspicious access?
- Do staff know how to report a suspicious email, login prompt or invoice request?
- Does the incident response plan explain who does what?
- Are cyber incidents included in wider business continuity planning?

Kevin added:

“A calm response does not happen by accident. It comes from planning, testing and making sure people know what to do before something goes wrong.

“Education cyber security should not be about blame or scare tactics. It should be about protecting learning, safeguarding information, reducing downtime and helping leaders communicate clearly when an incident happens.”