UK Edition

ThreatDown™
Powered by Malwarebytes

2025 Cybersecurity Guide for UK Education

Contents

Introduction

Schools, colleges, local authorities, academy trusts, and education service providers are faced with one of the toughest challenges in cybersecurity.

They must operate complex networks and safeguard sensitive data in a highly regulated environment—all while managing increasingly tight budgets. And they must protect students from online harm, mitigate a significant insider threat risk, handle enormous churn in their user population every year, and cater to the widely differing needs of both students and staff.

This combination of challenges makes educational institutions and their supply chains prime targets for ransomware gangs. IT and security staff working in the education sector must therefore be prepared to defend against organised, well-funded and highly experienced attackers.

This easy-to-use guide is designed to help educational institutions tip the scales back in their favour. It sets out the nature of the threats they face and their overarching compliance obligations, and it provides a simple risk assessment framework, an explanation of the tools they need to protect their environments, and a 10-step recovery plan to help them prepare for a breach.

Understanding the threat

According to the 2025 Cyber Security Breaches Survey by the Department for Science, Innovation & Technology, 44 per cent of primary schools, 60 per cent of secondary schools, 85 per cent of further education colleges, and 91 per cent of higher-education institutions in the UK identified a breach or attack in the past year.[1]

The most dangerous form of cyberattack is ransomware, and the scale of ransomware activity in the UK is highly significant:

- The UK suffers more ransomware attacks than any other country, apart from the USA, and between October 2022 and September 2024 its education sector was the hardest hit among G7 countries.[2]
- The UK's National Cyber Security Centre (NCSC) dealt with 430 incidents between September 2023 and August 2024 requiring its support, of which 317 were ransomware reports and 13 "nationally significant".[3]
- In May 2025, the Interlock ransomware gang attacked West Lothian Council's entire education network—covering 143 schools and nurseries—stealing millions of files containing information about teachers, parents, guardians, and students.
- Blacon High School in Cheshire was forced to close its doors to students for two days in January 2025 following a ransomware attack that disabled the school's IT systems and phone lines.
- In June 2024, the INC Ransomware group stole hundreds of gigabytes of internal documents from Cambridge University Press & Assessment, the organisation that manages Cambridge University's academic publications and worldwide exams.

UK schools are unprepared for a cyberattack

Cyber Essentials is a government-backed certification scheme recommended by the NCSC as the minimum standard of cybersecurity for all organisations. According to the Cyber security breaches survey 2025, only 20 per cent of primary schools and 43 per cent of secondary schools are even aware the scheme exists.

[1] Department for Science, Innovation & Technology (2025), Cyber security breaches survey 2025: education institutions annex, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-education-institutions-findings

[2] ThreatDown powered by Malwarebytes (2024), 2024 State of Ransomware Report, https://www.threatdown.com/dl-state-of-ransomware-2024/

[3] The Guardian (2024), UK underestimates threat of cyber-attacks from hostile states and gangs, says security chief, https://www.theguardian.com/technology/2024/dec/03/uk-underestimates-threat-of-cyber-attacks-from-hostile-states-and-gangs-says-security-chief

Understanding compliance obligations

UK schools, colleges and universities must comply with several laws and regulations that require strong cybersecurity protections.

Major regulations for UK educational institutions	Primary	Secondary	Further	Higher
Children Act 2004 (Section 11) Schools have an obligation to safeguard children, which includes keeping them safe from online harms.	✓	✓	✓	
KCSIE (Keeping Children Safe in Education) Schools and colleges must adopt cybersecurity measures such as filtering and monitoring, secure IT controls, and staff training.	✓	✓	✓	
Data Protection Act 2018 and UK GDPR Educational institutions must implement strict technical and organisational measures for processing personal data.	✓	✓	✓	✓
Privacy and Electronic Communications Regulations (PECR) Electronic communications activities, including providing Wi-Fi access, are subject to PECR rules and reporting obligations.	✓	✓	✓	✓
Counter-Terrorism and Security Act 2015 (Prevent Duty) Educational institutions must take steps to prevent radicalisation, including monitoring and filtering of extremist content.	✓	✓	✓	✓
Freedom of Information Act 2000 Public authorities must ensure secure information that may be subject to FOI requests and exemptions.	✓	✓	✓	✓
Equality Act 2010 Educational institutions must securely process and protect sensitive personal data related to protected characteristics.	✓	✓	✓	✓
Public Contracts Regulations 2015 Public institutions must follow secure procurement processes when purchasing cybersecurity solutions and services above threshold values.		✓	✓	✓
NIS Regulations 2018 and upcoming NIS 2 enhancements NIS regulations apply to organisations considered Operators of Essential Services, such as major research universities.				✓
Office for Students (OfS) conditions of registration Registered higher-education providers must maintain effective and integrated risk-management and cyber-resilience measures.				✓

Prevent: A simple risk assessment

To implement an effective cybersecurity strategy that provides safety and security, and supports their compliance efforts, it is essential that schools, colleges, universities, and education service providers understand the risks they face.

The following process provides a foundation for conducting a basic risk assessment. This assessment identifies critical assets, the threats they may encounter, and the potential consequences of failing to protect them.

Institutions are encouraged to document their findings thoroughly. Doing so not only demonstrates the methodology used but also allows for easier updates to the risk assessment in response to environmental changes or insights gained from security incidents.

Step	Action
1. Assets	Create a comprehensive inventory of your hardware, applications, user types, and stored data.
	Complete the action below for each asset identified in step 1.
2. Threats	Identify the threats that could harm the asset. Threats are things like password cracking, breaches, and ransomware.
3. Weaknesses	Identify weaknesses threats could exploit to cause damage, such as software vulnerabilities or weak password policies.
	Complete the actions below for each weakness identified in step 3. In determining risk, we recommend you weigh impact more heavily than likelihood, so you are adequately prepared for rare events with a severe impact, such as ransomware.
4. Likelihood	Decide how likely it is that this weakness will be exposed.
5. Impact	If the asset is lost or compromised, how would it affect your budget, compliance obligations, and core activities?
	Document the steps you have taken and the outcomes.

Protect: The essential security layers

Every education institution needs a set of essential security components—a mixture of documented policies, databases, hardware, network security solutions and endpoint protection.

Environment

Internet use policy	Asset management

Network

Email security	Next-gen firewall	Backup solution

Endpoints

The award-winning ThreatDown Education bundle delivers 10 layers of protection and safeguards Windows PCs, Chromebooks, Macs, and mobile devices.

Vulnerability assessment	Identify and prioritise weaknesses in the environment.
Patch management	Automated app and operating system updates.
Incident response	Automated endpoint remediation.
Next-gen AV	Best in class threat monitoring and isolation.
EDR	Award-winning Endpoint Detection and Response.
Device control	Prevent infection from peripherals.
Application block	Block unwanted applications.
Managed Threat Hunting	Identify and prioritise critical alerts 24/7.
Chromebook protection	Protect Chromebooks and Android mobile devices.
Ransomware rollback	Restore encrypted files up to 7 days after an attack.

Recover: A 10-step breach recovery plan

An institution's attack surface is constantly evolving as new individuals, devices, software, and data are introduced into the environment—and as cybercriminals adapt their tactics. Regardless of the number of protective measures in place, it is critical to remain prepared for the possibility of a security breach.

In the event of a breach, the following actions are recommended, in order:

1. Contain the attack	Isolate infected systems or networks to limit the impact of the attack.
2. Preserve evidence	In a serious attack you may be asked to preserve evidence for law enforcement, if you can.
3. Rollback if you can	Use ransomware rollback to restore systems to a known good state, if your solution allows.
	If you can't roll back
4. Understand the scope	Identify affected systems and data and prioritise critical systems for recovery.
5. Inform stakeholders	Inform senior leadership, PR, legal, cyber-insurance providers, security vendors and other stakeholders.
6. Seek assistance	Decide if you need expert assistance from law enforcement, vendors or other third parties.
7. Understand the breach	Identify compromised systems and accounts, and any persistence mechanisms left by attackers.
8. Rebuild	Use known good system images and backups to restore critical systems.
9. Reset, patch, upgrade	Reset passwords, patch vulnerable software, and implement missing security measures.
10. Learn what you can	Use what you have learned from the attack to improve your protection and policies.

Breaches can be extremely stressful. The individuals handling the incident should prioritise their actions, communicate clearly, take care of each other, and be encouraged to ask for help.

Learn more

The ThreatDown bundle for education is tailored for the needs of schools, colleges, universities, and service providers working in the education sector.

The bundle simplifies staff and student device protection with layers of award-winning protection:

- Attack surface reduction, next-gen AV, and Endpoint Detection & Response.
- Mobile security that unifies protection across Chromebook, iOS, and Android devices.
- 24x7x365 managed detection and response service.

And it delivers ease of use to minimize management effort and optimize performance:

- Single, cloud-based console for deployment, configuration, management, and reporting.
- Single, lightweight agent for the entire endpoint security stack.

Get started today >