Digital Security
Progress. Protected.

EDUCATION

PROTECTING EDUCATION: MEETING DFE CYBER STANDARDS WITH ESET

In today's digital learning environment, safeguarding sensitive data, systems and users has never been more important.

The Department for Education (DfE) has set out a series of cybersecurity standards to help schools and colleges strengthen their cyber resilience and reduce the risk of disruption caused by cyber attacks.

These standards cover key areas including user identity protection, threat detection, patch management, anti-malware defences and cyber awareness training.

ESET, a trusted cybersecurity provider with over 30 years of experience, offers a comprehensive suite of solutions that directly support schools and multi-academy trusts in meeting these DfE standards. Whether it's through advanced endpoint protection, phishing prevention, multi-factor authentication, or cyber training for staff and students, ESET enables education providers to meet their compliance responsibilities while staying one step ahead of cyber threats.

ESET IN EDUCATION – OUR COMMITMENT

- We protect over 1,200 schools.
- We protect over 271,000 devices for Education.
- Average seat count of education licenses is 225.
- Through our Safer Kids Online (https://www.saferkidsonlineng.com) initiative we worked with Internet Matters (https://www.internetmatters.org) to reach millions of teachers, parents and children in the UK helping them to stay safe whilst surfing the internet and we continue to deliver these important messages through our partnership with AFC Bournemouth.
- ESET's security blog welivesecurity.com has over 2 million subscribers worldwide and won the "European Vendor Cyber Security Blog of the Year" in 2024 for freely sharing threat intelligence and related information, to help make the internet a safer place.

CONTROL AND SECURE USER ACCOUNTS AND ACCESS PRIVILEGES

Protecting user accounts and related data is a critical line of defence against cyber incidents and attacks.

How ESET can help

ESET considers identity protection a cornerstone of cyber defence. Our layered approach includes:

- **ESET Cloud Office Security (ECOS):** Shields inboxes from phishing campaigns before emails reach the user.
- **Endpoint Protection:** Detects malicious email links and files using heuristics, AI and phishing filters.
- **ESET Secure Authentication (ESA):** Provides multi-factor authentication (MFA/2FA) for cloud (e.g., M365), local login, VPN and remote desktop access using OTP, push notifications, SMS, hardware tokens, or email.
- **FIDO2 & Passkey Support:** Enhances MFA with passwordless authentication.
- **ESET MDR (Managed Detection and Response):** Detects and neutralises compromised accounts engaging in 'living off the land' attacks, supporting rapid account suspension and recovery.

CREATE AND IMPLEMENT A CYBER AWARENESS PLAN FOR STUDENTS AND STAFF

Well-informed users are the best line of defence against cyber criminals. Many cyber incidents and attacks target common processes and human behaviours when using digital technology.

Raising awareness, and training students and staff on cyber security will:

- Reduce the risk of cyber incidents and attacks
- Help to keep students and staff safe
- Help to create a culture where students and staff feel comfortable identifying and reporting risk
- Help students and staff understand what acceptable use of digital technology looks like and the importance of cyber security – this can help inform behaviour policies
- Make sure that cyber incidents, attacks and risks are reported quickly to stop them spreading

How ESET can help

- **ESET Cybersecurity Awareness Training (ECAT)**
- **Phishing Simulations:** Real-world email testing with feedback for continual improvement.
- **Safer Kids Online:** Engaging resources and guidance to support younger users and their families in staying safe online.

LICENCE DIGITAL TECHNOLOGY AND KEEP IT UP TO DATE

- All digital technology must be properly licensed. This includes software programmes, operating systems, and applications running on devices and servers, as well as cloud-based services.

- IT support must complete security updates (known as patching) to operating systems, applications and firmware, including configuration changes, within 14 days of the release of the patch where the vulnerability is:
  - described as high risk or worse
  - has a Common Vulnerability Scoring System (CVSSv3) score of 7 or above – you should also triage and prioritise updates for other scores when it is possible to do so

How ESET can help

- **ESET PROTECT Platform:** Creates a full inventory of all licensed digital assets.
- **Vulnerability & Patch Management (V&PM):** Identifies and mitigates known software vulnerabilities.
- **Automated Patching:** Background installation of updates to Windows, with MacOS and Linux support forthcoming.
- **Integrated Threat Defence:** Combines patching with anti-exploit technology and MDR response, offering comprehensive risk management.

SECURE DIGITAL TECHNOLOGY AND DATA WITH ANTI-MALWARE AND A FIREWALL

Creating and maintaining the security around your digital technology and data is a critical line of defence against a cyber incident or attack. Once a virus or hacker is in your system, they will look for a way to exploit other vulnerabilities.

How ESET can help

Anti Malware and endpoint firewalls are products that ESET has been providing to customers for decades. Whilst the DfE standard recommends a boundary firewall, which we would agree with, it's important that staff and students working remotely on school equipment have the network boundary move with them and an endpoint firewall extends the protection of this. We have also seen in a number of instances, attackers penetrating inside a network, and being able to bypass a boundary firewall and therefore we would consider endpoint firewalls a critical part of protection.

- **ESET Endpoint Protection:** Delivers real-time protection through AI, machine learning and HIPS (Host Intrusion Prevention System).
- **ESET LiveGuard Advanced:** Uses cloud-based sandboxing to pre-emptively block zero-day threats.
- **ESET MDR (Managed Detection and Response):** Provides 24/7 monitoring by cyber experts who proactively hunt for threats, analyse suspicious activity, and respond swiftly to incidents — including those involving highly skilled and persistent threat actors.
- **ESET Cloud Office Security:** Integrates with M365 and Google Workspace to protect Exchange, OneDrive, SharePoint, Teams, Gmail and Google Drive.
- **Endpoint Firewall:** Enforces granular firewall rules, supports IDS/IPS and inherits policies from Windows Group Policy for seamless deployment in remote or hybrid environments.

MONITOR DEVICES, APPLICATIONS AND SERVICES FOR UNUSUAL ACTIVITY AND SIGNS OF COMPROMISE

Continuous monitoring is essential to detect early indicators of attack and prevent widespread disruption. The DfE highlights the importance of logging, monitoring access attempts, documenting policy decisions and using tools capable of identifying suspicious behaviour and privilege escalation.

How ESET can help

- **ESET Inspect (EDR):** Provides deep visibility into endpoint activity, identifying abnormal behaviours, privilege escalations and lateral movement attempts across the network.
- **ESET PROTECT Console:** Centralises event logging, risk scoring and real-time notifications for all endpoints. Logs are securely stored and can be used to support audit and compliance reporting.
- **ESET LiveGrid® Reputation System:** Helps administrators assess application risk using community-based threat intelligence.
- **Policy Documentation and Enforcement:** All firewall, access and control policies within ESET products can be centrally configured, enforced and documented, ensuring transparent and traceable decision-making aligned with DfE expectations.

REPORT CYBER ATTACKS

A cyber incident or attack will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college.

Everyone is responsible for and should report a cyber incident or attack to their IT support and senior leadership (SLT) digital lead.

How ESET can help

- **ESET MDR:** Provides 24/7/365 monitoring and response with an average intervention time of under 20 minutes.
- **Digital Forensics & Incident Response (DFIR):** Delivers insights into the origin and behaviour of attacks.
- **Automated Containment:** Limits the spread of threats before users even realise a breach has occurred.

ESET protect tiers

Scalable and customisable security subscriptions, easy to manage from a cloud or on-prem console.

	PROTECT MDR ULTIMATE	PROTECT MDR	PROTECT ELITE	PROTECT ENTERPRISE	PROTECT COMPLETE	PROTECT ADVANCED	PROTECT ENTRY
PLATFORM MODULES							
CONSOLE (CLOUD/ON-PREM)	●	●	●	●	●	●	●
MODERN ENDPOINT PROTECTION (WITH NGAV)	●	●	●	●	●	●	●
SERVER SECURITY	●	●	●	●	●	●	●
MOBILE THREAT DEFENCE	●	●	●	●	●	●	○
FULL DISK ENCRYPTION	●	●	●	●	●	●	
ADVANCED THREAT DEFENCE	●	●	●	●	●	●	
VULNERABILITY & PATCH MANAGEMENT	●	●	●	○	●	○	○
MAIL SERVER SECURITY	●	●	●	○	●	○	○
CLOUD APP PROTECTION	●	●	●	○	●	○	○
EXTENDED DETECTION AND RESPONSE	●	●	●	●			
MULTI-FACTOR AUTHENTICATION	●	●	●	○	○	○	○
SERVICES							
TECHNICAL SUPPORT	●	●	●	●	●	●	●
MDR SERVICE		●	○	○			
MDR ULTIMATE SERVICE	●		○	○			
PREMIUM SUPPORT		●	○	○	○	○	○
PREMIUM SUPPORT ULTIMATE	●	○	○	○	○	○	○
ADD-ONS & EXTRAS							
ESET AI ADVISOR	●	○	○	○			
THREAT INTELLIGENCE FEEDS & REPORTS	○	○	○	○	○	○	○
SHAREPOINT SECURITY	○	○	○	○	○	○	○
ENDPOINT ENCRYPTION	○	○	○	○	○	○	○
CYBERSECURITY AWARENESS TRAINING	○	○	○	○	○	○	○

● Included ○ Optional

How ESET Protect tiers help you comply with DFE standards

	CYBER AWARENESS TRAINING	PROTECT MDR	PROTECT COMPLETE	PROTECT ADVANCED	PROTECT ENTRY
SECURE DIGITAL TECHNOLOGYAND DATA WITH ANTIMALWARE AND A FIREWALL		●	●	●	●
MONITOR DEVICES, APPLICATIONS AND SERVICES		●	●	●	●
LICENCE DIGITA TECHNOLOGY AND KEEP IT UP TO DATE		●	●		
CONTROL AND SECURE USER ACCOUNTS AND ACCESS PRIVILEGES		●	●		
REPORT CYBER ATTACKS		●			
CREATE AND IMPLEMENT A CYBER AWARENESS PLAN	●				

Digital Security
Progress. Protected.

For more information please contact:

ESET:
sales@eset.co.uk
www.eset.com/uk/