SOPHOS

Safeguarding Requirements in Education

Achieving Digital Safeguarding and Cyber Resilience with Sophos

A Sophos Whitepaper. March 2024

Introduction

The UK Department for Education (DfE) provides statutory guidance issued under Section 175 of the Education Act 2002 (as amended), the Education (Independent School Standards) Regulations 2014, the Non-Maintained Special Schools (England) Regulations 2015, and the Apprenticeships, Skills, Children and Learning Act 2009 (as amended). Schools and colleges in England must have regard to this guidance when carrying out their duties to safeguard and promote the welfare of children.

Safeguarding the welfare of young learners and the technological solutions used to do so must then be considered as part of the wider requirements mandated by DfE to meet the 12 digital and technology standards in schools and colleges[1], which mandate some basic requirements on IT infrastructure to protect the educational environment from cyber-attacks:

- "Protect all devices on every network with a properly configured boundary or software firewall.
- Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date.
- Accounts should only have the access they require to perform their role and should be authenticated to access data and services.
- You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication.
- You should use anti-malware software to protect all devices in the network, including cloud-based networks.
- An administrator should check the security of all applications downloaded onto a network.
- All online devices and software must be licensed for use and should be patched with the latest security updates.
- You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off-site.
- Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber attack.
- Serious cyber attacks should be reported.
- You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by General Data Protection Regulation.
- Train all staff with access to school IT networks in the basics of cyber security."

DFE DIGITAL AND TECHNICAL REQUIREMENT	SOPHOS RECOMMENDED SOLUTION
Protect all devices on every network with a properly configured boundary or software firewall.	**Sophos Firewall** At school network boundary. **Sophos Intercept X Advanced** Manage / monitor the Windows Client Firewall.
Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date.	**Sophos Firewall** At school network boundary. **Sophos Network Detection and Response** Part of Sophos Extended Detection and Response (XDR) and Sophos Managed Detection and Response (MDR) licences to identify unknown devices and provide an intrusion prevention system to help protect against compromise.
Accounts should only have the access they require to perform their role and should be authenticated to access data and services.	**Sophos Intercept X Advanced** **Sophos XDR / MDR** Monitors event logs for user logins and can be used to determine inappropriate use.
You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication.	**Sophos XDR with Integration Pack** All Sophos solutions use multi-factor authentication (MFA) to secure access for administrators, and Sophos XDR and Sophos Managed Detection and Response (MDR) integration packs consume data from Identity providers to help identify inappropriate use.

1 https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges

DFE DIGITAL AND TECHNICAL REQUIREMENT	SOPHOS RECOMMENDED SOLUTION
You should use anti-malware software to protect all devices in the network, including cloud-based networks.	**Sophos Intercept X Advanced** Provides industry leading threat protection for all Windows, mac workstations and Windows servers and Linux servers within the network or cloud environments (such as AWS or AZURE)
An administrator should check the security of all applications downloaded onto a network.	**Sophos Firewall** Web Downloads / Application Control. **Sophos Intercept X Advanced** Manage / monitor applications through Application Control and Server Lockdown.
All online devices and software must be licensed for use and should be patched with the latest security updates.	**Sophos Firewall** Web Downloads / Application Control. **Sophos Intercept X Advanced XDR** Collects lists of installed applications and versions for comparison with Common Vulnerabilities and Exposure (CVE) databases.
Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber attack.	**Sophos Professional Services** Table Top Exercises to help environments develop and test disaster recovery (DR) / incident response (IR) contingency plans.
Train all staff with access to school IT networks in the basics of cyber security.	**Sophos Phish Threat** Provides regular phishing training for staff.

School governing bodies must implement solutions to comply with these mandated requirements while also factoring in technology, policies and procedures for safeguarding and welfare. School leaders should ensure there are appropriate policies and procedures in place for appropriate action to be taken in a timely manner to safeguard and promote children's welfare. These policies should include individual schools and colleges having an effective child protection policy which:

- reflects reporting systems (safeguarding policies and procedures)
- includes policies, such as online safety
- is reviewed annually (as a minimum) and updated if / when needed.

This white paper particularly refers to:

Department for Education Keeping Children Safe in Education (KCSIE) 2023[2], published 1st September 2023; Department for Education Meeting Digital and Technology Standards in Schools and Colleges[3], published 23rd March 2022, updated 29th March 2023; and the UK Government's Prevent Duty Guidance: England and Wales (2023)[4] published 2nd March 2015, Updated 14th September 2023.

The Welsh and Scottish Governments have similar legislation that is also included within this white paper, and where applicable this document also references:

> The Welsh Government Wales Safeguarding Procedures – Safeguarding Children from Online Abuse, last updated February 2021[5] and Enhancing Digital Resilience in Education[6]; and the Hwb Keeping Safe Online resources[7] and The Wales Safeguarding Procedures for Children and Adults at Risk of Abuse and Neglect[8&9].
>
> The Scottish Government, Education Scotland's Child Protection and Safeguarding Policy (Feb 2021)[10]; Getting it Right for Every Child (GIRFEC) and the Children and Young People (Scotland) Act place a duty on schools and local authorities to safeguard and promote the welfare of all children[11].

The statutory guidance uses the terms "must" and "should" throughout. It uses the term "must" when the person in question is legally required to do something and "should" when the advice set out should be followed unless there is good reason not to.

2 https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
3 https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges
4 https://www.gov.uk/government/publications/prevent-duty-guidance/prevent-duty-guidance-for-england-and-wales-accessible
5 https://safeguarding.wales/en/chi-i/chi-i-c6/c6-p6/
6 https://www.gov.wales/enhancing-digital-resilience-education
7 https://hwb.gov.wales/keeping-safe-online
8 https://safeguarding.wales/en/int-i/int-i-i1/i1-p1/
9 https://safeguarding.wales/en/chi-i/chi-i-c6/c6-p6/
10 https://education.gov.scot/media/dkxhqhwz/child-protection-and-safeguarding-policy-es-feb21.pdf
11 https://www.legislation.gov.uk/asp/2014/8/contents/enacted

This white paper has been written to help schools and colleges understand the current Department for Education guidance on protecting learners from online content, and where Sophos solutions can assist. It will help the school Senior Leadership Team (SLT), Designated Safeguarding Leader (DSL) (or Designated Senior / Safeguarding Person, (DSP) in Wales) and IT Teams understand what technical solutions they require to help provide evidence to Ofsted that the education setting has an effective safeguarding policy and reporting procedures.

As noted above, this white paper is primarily focused on DfE and Ofsted requirements for safeguarding. Educational establishments must also consider the wider context of cyber security as part of their safeguarding solution to protect other areas within the environment from physical / online attack, compromise, ransomware attack or data theft.

The amount of Personally Identifiable or Sensitive Personally Identifiable Information held within these settings on servers, desktops, laptops, tablets, and increasingly within public cloud infrastructure such as Azure, Amazon Web Services (AWS), or Google Cloud is phenomenal. For example, student medical or criminal information, scans of teachers' passports or driver's licences, postal addresses, contact details for next of kin, and bank or credit card information for cashless payments all are worth significant amounts of money to threat actors.

Schools, colleges, and higher / further education establishments are regularly targeted by threat actors[12]. The recent Sophos State of Ransomware 2023 report reveals that 80% of respondents from educational settings admitted to having at least one ransomware attack in the last 12 months.

Looking specifically at education environments, 36% of the attacks came from compromised credentials, 29% from the exploitation of vulnerabilities, and 19% from malicious emails. Looking back to the DfE 12 standards, these are areas that are mostly covered by the requirements set out in this document.

Threat actors operate 24x7, however IT support in most educational establishments operates office hours with very limited support out of hours, over weekends, or during holidays. This leaves the computing estate vulnerable to compromise, data theft, and ransomware while left effectively unattended.

According to research by Gartner and industry analysts, for effective cyber security at least five dedicated threat hunters are required to provide true 24x7x365 coverage within a security operations team. This is in addition to the IT staff required for business-as-usual activities.

Most environments typically have at least 10 separate point solutions used in some capacity for cyber security – endpoint protection, patching, MFA, unified endpoint management (UEM) / mobile device management (MDM), Microsoft 365, firewall, zero trust network access (ZTNA) / virtual private network (VPN), network monitoring, System Center Configuration Manager (SCCM) / Active Directory (AD) etc. Unfortunately, in 2023/24 these solutions typically result in log overload.

Over the last few years, many companies have seen security information and event management (SIEM) solutions as the answer, with their expensive ability to consume logs in lots of different formats and little to no ability to normalize or standardize into a common format. As a result, they are great at consuming data but less effective at cyber security and hunting for signs of compromise.

The only viable option is a truly integrated solution, such as Sophos Central. It allows the use of different protection products (depending on the licence) while providing a central secure data lake. This allows for a common data structure and intelligent threat hunting of suspicious indicators of compromise or unaccountable events, regardless of whether the event is email, endpoint, identity, firewall, network or Microsoft 365 / public cloud-based. Educational establishments need to consider a holistic integrated approach not only to safeguarding but also to cyber security and threat protection.

12 https://www.sophos.com/en-us/content/state-of-ransomware

The Education Inspection Framework

The Education Inspection Framework[13] and Ofsted Inspection Handbook[14] sets out how Ofsted inspects maintained schools, academies, non-association independent schools, and further education institutions in England. The Independent Schools Inspectorate (ISI)'s inspection framework sets out how it inspects independent schools in England, including residential (boarding) schools and registered early years settings:

"34. We expect schools to meet the other requirements of Keeping children safe in education, but have no additional or separate expectations of schools concerning:

- using a digital platform to monitor pupils' internet use, and we do not specify how these platforms should operate.

[...]

378. All schools should have an open and positive culture around safeguarding that puts pupils' interests first. This means they:

- protect pupils from serious harm, both online and offline
- are vigilant, maintaining an attitude of 'it could happen here'
- are open and transparent, sharing information with others and actively seeking expert advice when required
- ensure that all those who work with pupils are trained well so that they understand their responsibilities and the systems and processes that the school operates and are empowered to 'speak out' where there may be concerns
- actively seek and listen to the views and experiences of pupils, staff, and parents, taking prompt but proportionate action to address any concerns, where needed
- have appropriate child protection arrangements, which:
- identify pupils who may need early help, and who are at risk of harm or have been harmed. This can include but is not limited to, neglect, abuse (including by their peers), grooming, exploitation, sexual abuse, and online harm
- secure the help that pupils need and, if required, refer in a timely way to those who have the expertise to help
- manage safe recruitment and allegations about adults who may be a risk to pupils
- are receptive to challenge and reflective of their own practices to ensure that safeguarding policies, systems and processes are kept under continuous review.

[...]

419. Inspectors will always consider the effectiveness of the school's safeguarding."14

Prevent Duty

Inspectors will evaluate the extent to which the setting has a culture of safeguarding that supports effective arrangements to identify learners who may need early help or who are at risk of harm or exploitation, including radicalization. For Ofsted and ISI, this forms part of the leadership and management judgment. Governors, in particular, must ensure that the school's arrangements for safeguarding meet statutory requirements.

13 https://www.gov.uk/government/publications/education-inspection-framework
14 https://www.gov.uk/government/publications/school-inspection-handbook-eif/school-inspection-handbook-for-september-2023

Achieving Digital Online Safeguarding

Keeping Children Safe in Education (KCSIE) 2023

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

Increasingly with remote settings (for example remote learning during Covid), schools and colleges need to consider the safety of pupils, students, and staff while remote learning. Technologies like client-based web filtering and zero trust networking can assist with building a robust cyber security policy.

Filtering and monitoring are a fundamental responsibility to safeguard and limit children's exposure to the four categories of risk (Content, Contact, Conduct, and Commerce – 4Cs). As part of this process, governing bodies should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness.

The appropriateness of any filtering and monitoring systems is a matter for individual schools and colleges and will be informed, in part, by the risk assessment required by the Prevent guidelines. However, schools and colleges must have effective monitoring strategies in place that meet their safeguarding needs.

Ninety percent of all network and internet traffic is encrypted. To comply with DfE guidelines both HTTP and HTTPS filtering must be carried out to ensure that effective filtering and monitoring is achieved.

To support schools and colleges, the DfE has published the Filtering and Monitoring Standards Additional guidance on "appropriate" filtering and monitoring can be found at: UK Safer Internet Centre[15] and in particular the Sophos Firewall 2023 Vendor Response[16].

KCSIE 2023 Appendix B also contains a section relating to cybercrime and highlighting the impact on education settings or third parties where computers can be used to compromise computer networks / corporate environments. Schools and colleges contain a significant volume of Personally Identifiable or Sensitive Personally Identifiable Information (for example student medical records, copies of passport / driving licence details for teachers or staff who may drive the school minibus, or arrange activities such as trips abroad).

Educational establishments are regularly targeted by threat actors and require a robust 24x7 detection and response system, such as Sophos Managed Detection and Response as part of their cyber risk mitigation strategy.

The Prevent Duty should be seen as part of schools' and colleges' wider safeguarding obligations. The guidance is set out in terms of four general themes: risk assessment, working in partnership, staff training, and IT policies.

Filtering and monitoring standards for schools and colleges

Schools and colleges should provide a safe environment, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

There are several technical requirements that the Senior Leadership Team (SLT) is responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of the provision
- overseeing reports.

15 https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring
16 https://d1xsi6mgo67kia.cloudfront.net/uploads/2022/12/Sophos-Appropriate-Filtering-Provider-Response-Sophos-2023.pdf

The SLT should work closely with the Designated Safeguarding Leader (DSL) and IT providers in all aspects of creating a robust filtering and monitoring policy within the educational setting. As part of these requirements training may be required by the DSL and IT Team to ensure that the filtering solution is set up and configured correctly.

The DSL should take lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems.

The IT service provider should have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems.

The IT service provider should work with the SLT and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks.

The filtering system should be operational, up to date, and applied to all:

- users, including guest accounts

Sophos Compliance Status: Fully Compliant
Guest users are users who don't have an account within the school's User Authentication Directory (Microsoft AD or Azure AD or locally within the firewall) and want to connect to your school network to access the internet. You can register guest users or allow them to register through the guest user portal. You can print credentials or send them through SMS.

After authentication, the guest user is granted access according to the selected policies or is redirected to the Sophos Firewall captive portal. This is a web page that requires users behind the firewall to authenticate when attempting to access a website or the internet.

- school owned devices

Sophos Compliance Status: Fully Compliant
Sophos Firewall supports both NTLM (NT LAN Manager) and Kerberos authentication.

Sophos Transparent Authentication Suite (STAS) enables users on a Windows domain to sign in to Sophos Firewall automatically when signing in to Windows. This eliminates the need for multiple sign-ins and for single sign-on (SSO) clients on each client device.

For customers using the Sophos Intercept X Advanced endpoint protection client, the Security Heartbeat is also available as a user authentication method. When a user signs in to an endpoint, Security Heartbeat sends a synchronized user ID containing the domain name and username to Sophos Firewall. Sophos Firewall checks the user account with the configured Active Directory server and activates the user.

- devices using the school broadband connection

Sophos Compliance Status: Fully Compliant
The Sophos Firewall typically sits on the boundary between the internet / internet service provider (ISP) connection and the educational establishment's internal networks and demilitarized zone (DMZ).

All IPv4 and IPv6-based network traffic is then filtered at this point as per the policies set within the Firewall for inbound / outbound traffic.

Your filtering system should:

- filter all internet feeds, including any backup connections

Sophos Compliance Status: Fully Compliant
Sophos Firewall typically sits on the boundary between the internet / ISP connection and the educational establishment's internal networks and DMZ.

All IPv4 and IPv6-based network traffic is then filtered at this point as per the policies set within the Firewall for inbound / outbound traffic.

Sophos Firewall also natively supports Transport Layer Security (TLS) 1.3, providing a robust filtering solution for the latest HTTPS encryption and cyphers, and mobile device certificate pinning.

- be age and ability appropriate for the users, and be suitable for educational settings

Sophos Compliance Status: Fully Compliant
The flexible nature of the web filtering policies within the Sophos Firewall allows educational settings to set up and apply specific policies to different users, groups of users, or devices, allowing granular policy controls to be configured as appropriate to age and educational learning requirements.

- handle multilingual web content, images, common misspellings, and abbreviations

Sophos Compliance Status: Fully Compliant
Sophos produces and sells Sophos Firewall around the world and will fully support multilingual web content, images, misspellings, and abbreviations.

The management console supports administration in Default English, Chinese Simplified, Chinese Traditional, Hindi, French, German, Italian, Korean, and Brazilian Portuguese.

- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them

Sophos Compliance Status: Fully Compliant
Sophos Firewall is designed as an industry-leading cyber security solution that includes many web browsing categories, including anonymizing web proxies.

Within application control, you can also apply bandwidth restrictions and restrict traffic from applications (such as VPN) which can be used to bypass security / safeguarding protections or lower productivity. Application filters allow you to control traffic by category or on an individual basis. With synchronized application control, you can restrict traffic on endpoints that are managed with Sophos Central. Managing cloud application traffic is also supported.

- provide alerts when any web content has been blocked

Sophos Compliance Status: Fully Compliant
Sophos Firewall includes real-time in-depth reporting and scheduled email alerting to provide DSL and IT Teams with alerts relating to search engine use, blocked web attempts, web content, etc.

Granular Role Based Administration on the Firewall allows DSLs to be set up with a limited "Firewall Audit" Administration role, which allows access to real-time logs and reporting if required by the educational setting's safeguarding policy.

Mobile and app content is often presented in a different way to web browser content. If your users access content in this way, you should get confirmation from your provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.

Sophos Compliance Status: Fully Compliant
Sophos Firewall also natively supports TLS 1.3, therefore providing a robust filtering solution for the latest HTTPS encryption and cyphers, and mobile content provided to devices using certificate pinning.

It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the SLT or the DSL.

Your filtering systems should allow you to identify:

- device name or ID, IP address, and where possible, the individual

Sophos Compliance Status: Fully Compliant
The logging within the Sophos Firewall includes the user information, device details, and IP address.

- the time and date of attempted access

Sophos Compliance Status: Fully Compliant
All logging and reporting data is date and time-based.

- the search term or content being blocked

Sophos Compliance Status: Fully Compliant
The Sophos Firewall includes real-time in-depth reporting and scheduled email alerting to provide DSL and IT Teams with alerts relating to search engine use, blocked web attempts, web content, etc.

Granular Role Based Administration on the Firewall allows for DSLs to be set up with a limited "Firewall Audit" Administration role, which allows access to real-time logs and reporting if required by the educational setting's safeguarding policy.

Conclusion

Sophos offers a complete cyber security solution for customers in all sectors to protect them from modern cyber threats. It also offers a single platform for extended detection and response – the Sophos delivered Managed Detection and Response services – which will help educational establishments meet the 12 DfE cyber security / technology requirements, helping to reduce any cyber insurance costs while also meeting the DfE requirements for safeguarding children in education.

Sophos Firewall is an industry-leading cyber security solution. It fully complies with the UK Department for Education KCSIE 2023, Prevent Duty and DfE Filtering and Monitoring requirements needed by educational settings to safeguard learners from inappropriate material (4Cs).

As an integral part of the Sophos Cybersecurity Ecosystem, Sophos Firewall is available as a clustered solution and will fully integrate into the Sophos Central Management platform to provide a single, integrated solution for all educational environment cyber security needs.

Increasingly, cyber attackers operate 24x7, so a truly integrated solution with the option of Sophos Managed Detection and Response provides customers with the reassurance that over 500 Sophos Threat Experts are watching over the security of their environments and preventing compromise from hackers, ransomware, or malware – all while safeguarding learners from accessing inappropriate websites, web content, or applications.

2024-03-08 (WP-NP)

SOPHOS