

breathetechnology
support | cloud | security | infrastructure | comms

HELPING SCHOOLS MEET
**The DfE's Digital
& Technology
Standards**



SONICWALL® SHOP
A Breathe Technology Business

DfE School Guidance

Meeting Digital and Technology Standards, as well as Cyber Security Standards in Schools

Is your school meeting the DfE's Digital and Technology and Cyber Security Standards?

In March 2023, the Department for Education updated their guidance to schools regarding how to meet digital and technology standards. This standard specifies the minimum requirements to consider when renewing and upgrading digital infrastructure and the requirements for cyber security, user accounts and data protection.

Meeting the DfE digital and technology standards can help you make more informed decisions about technology leading to safer, more cost-efficient practices and new learning opportunities for students.

The standards can help your school with:

- Budgeting for technology procurement and maintenance
- Buying technology equipment and services
- Renewing a contract with a technology provider to ensure their purchases meet your needs
- Correctly installing new equipment

Many of these standards should be implemented when

you next upgrade your digital infrastructure. However, some of the standards, such as filtering, monitoring and safeguarding should already be in place. Others are highly recommended for immediate action such as cyber security and broadband, while some may take years to implement when your current solutions are underperforming or unsupported.

At Breathe Technology, we can assess your current provision and advise which actions need to be taken in order to ensure compliance with each standard, from there we can implement the suggested improvements and upgrades to fulfill these requirements.

The DfE set out eight categories your school needs to meet:

1
CYBER
SECURITY

2
BROADBAND

3
WIRELESS
NETWORK

4
NETWORK
SWITCHING

5
FILTERING &
MONITORING

6
CLOUD
SOLUTIONS

7
NETWORK
CABLING

8
SERVERS &
STORAGE

1 CYBER SECURITY

Is your school meeting the DfE's Cyber Security Standards?

The education sector is under increasing pressure to ensure the effective practice of cyber security measures. When cyber security incidents occur, they impact the day-to-day running of schools, lead to sensitive data loss and cause reputational damage.

Implementing the DfE's Cyber Security Standards will protect your school from threats and prepare your school should a cyber security incident occur. At Breathe Technology, we are able to work with your school to fulfill the DfE cyber security standards.

The DfE set out twelve requirements your school needs to meet:

1. Protect all devices on every network with a properly configured boundary or software firewall.

Having a properly configured boundary or firewall in place will prevent many cyber attacks. They also make scanning for suitable hacking targets much harder.

2. Network devices should be known and recorded with their security features enabled, correctly configured and kept up to date.

Attackers will exploit devices where the security features are not enabled. Attackers who gain physical access to a network device can exploit a system much more easily, so this should be prevented. Recording network devices helps schools keep networks up-to-date and speeds up recovery.

3. Accounts should only have the access they require to perform their role and should be authenticated to access data and services.

Successful cyber attacks will target the user accounts that have the widest access and highest privileges on a network. If you prevent and limit the compromise of these accounts, you prevent and limit successful cyber attacks.

4. You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication.

Multi-factor authentication reduces the possibility of an attacker compromising an account by using two types of authentication forms. This is especially important if an account has access to sensitive or personal data that could have a serious impact on the establishment, staff or students.

5. You should use anti-malware software to protect all devices in the network, including cloud-based networks.

Up-to-date anti-malware and anti-virus software reduces the risk from many forms of cyber attack. Some applications protect against viruses and general malware, some against one only. Your school needs to protect against both.

6. An administrator should check the security of all applications downloaded onto a network.

Applications may contain unintentional security flaws or introduce malware onto a network, making it simpler to carry out an attack. Therefore, applications should not be downloaded by users, they should first be examined by the IT service provider.

7. All online devices and software must be licensed for use and should be patched with the latest security updates.

Hackers will try to identify and exploit the vulnerability that each new security update addresses. They try to do this before users can update their systems. Unsupported software will not receive security updates and over time it becomes more vulnerable and less compatible with the security measures integrated into the network.

You must not use unlicensed hardware or software. Unlicensed software may not be a legitimate copy, or it may not be updatable to the latest secure standards.

8. You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off-site.

A backup is a second copy of data that is kept in a different place in case the first copy is lost or damaged, this is essential for disaster recovery in the event of a disaster. The safest way to do this is to establish a pattern of backing up on a rolling schedule. When not in use, you should keep these backups off the network and periodically check them.

9. Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber-attack.

Remaining unprepared for a cyber attack can lead to poor decisions, slow recovery, and expensive mistakes. A good response strategy made ahead of time will help you respond quickly, calmly, and efficiently. Effective response will reduce the material, reputational and safeguarding damage from ransomware attacks.

10. Serious cyber-attacks should be reported.

You should report any suspicious cyber incident to Action Fraud on 0300 123 2040 or on the Action Fraud website. Police investigations may find out if any compromised data has been published or sold and identify the perpetrator.

11. You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by General Data Protection Regulation.

The protection of sensitive and personal data is vital to the safety of staff and students, the school reputation, and the legal liabilities that security breaches will expose schools to.

12. Train all staff with access to school IT networks in the basics of cyber security.

The most prevalent types of cyber attacks depend on human error to be successful. Attacks can be stopped by avoiding these mistakes. Basic cyber security knowledge amongst staff and governors is vital in promoting a more risk aware school culture.

When should you meet the standards?

All standards should be implemented as soon as possible, and you should already be meeting several standards, particularly in relation to the data protection regulations. With cover for cyber security incidents now added to the threats covered by the RPA, meeting these standards will also help you comply to the conditions of your cover.

How can we help?


We are able to guide your school through these guidelines and help you implement a cyber security strategy most suitable for your school. We can help assess your school's cyber resilience, prioritise critical risks, back up your data, provide assurance and achieve network security.

When your school is ready to enhance your network and adhere to DfE standards, Breathe Technology will be here to guide you through it.


COMPANY OVERVIEW

Boundless Cybersecurity for the Hyper-Distributed Era


FOUNDED 1991 HEADQUARTERS Milpitas, California EMPLOYEES 1,600+ WWW.SONICWALL.COM




Global Footprint
500,000+ customers in 215 countries and territories




Industry Veteran
Trusted 30-year veteran of the cybersecurity industry




End-to-End Portfolio
Comprehensive cybersecurity product and service platform



Global Threat Intelligence Network
Hundreds of terabytes, artifact threat data

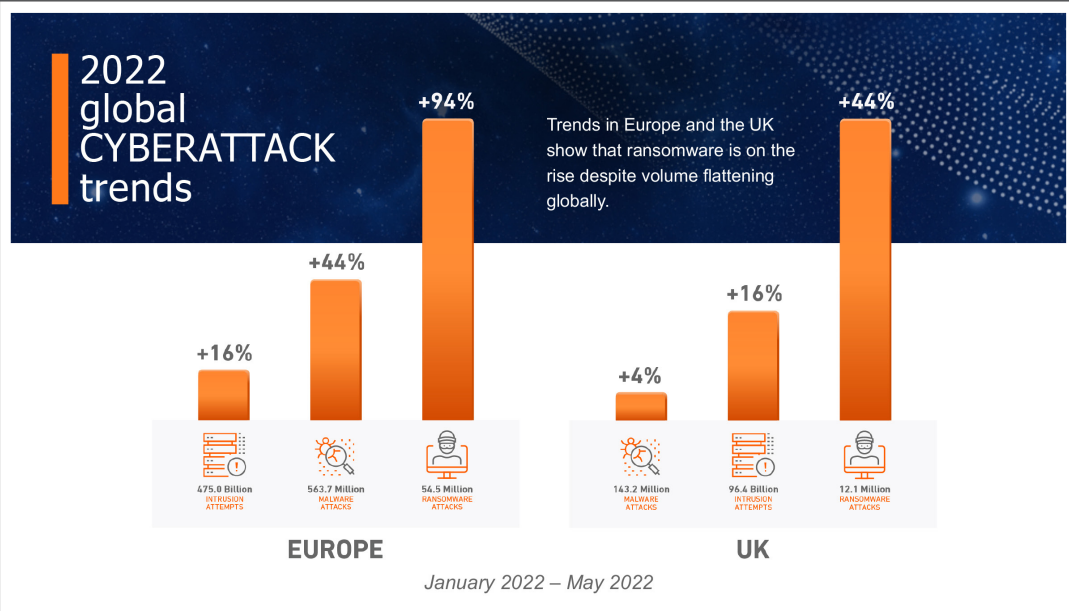


100% Channel
17,000+ global channel partners



Cybersecurity Innovation
More than 300 innovative patents granted, including RTDMI™

SONICWALL



BREATHE TECHNOLOGY AND SONICWALL

20 Years of Collaboration



Gold Accredited Partner

- Must hold required technical certifications (renewed every 2 years)
- Must meet annual revenue goals
- Must meet annual learning criteria
- Joint business planning



Industry Veteran


Trusted 20-year veteran of the SonicWall Community



Technical Excellence

- One of the lowest support case to customer base ratios in the UK
- Knowledgeable Support desk
- Safe pair of hands

SONICWALL




As an Education specialist IT Provider, Breathe in collaboration with Sonicwall would like to help, make it easier for schools, to benefit from this technology and to meet the guidelines.

The following is available to you:

1. Free of charge security risk analysis
2. Free demonstration of the products and discussion on your security and safeguarding currently in place
3. Heavily discounted pricing and trade in programme on old Firewall/Webfilter hardware. Meaning you get something back on old systems that would normally have no resale value.

(Get the hardware free when purchasing the standard 3 year license/ warranty)

 www.breathetechnology.com
(live chat available)

 **London** 020 3519 0124
Cambridge 01223 209920
Sheffield 0114 349 8054

 lucy@breathetechnology.com

breathetechnology
support | cloud | security | infrastructure | comms