

**breathe**technology  
support | cloud | security | infrastructure | comms

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



# DfE Technology Standards

## *Meeting Digital Standards*

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



Craig Van Aswegen  
MD & Snr IT  
Management Consultant  
Breathe Technology LTD

The Department for Education has updated their guidance to schools regarding how to meet digital and technology standards.

*"This means that your school must understand and update all your procedures to comply to these changes, which will lead to safer, more cost-efficient practices with new learning opportunities.*

Whether you **already have an in-house IT team, out-source your IT or just need a little helping hand** with these changes, **we are here to help in whatever way you require."**



# Content

<b>1</b>	<b>CYBER SECURITY</b> .....	<b>1</b>
	Cyber Security, User Accounts, Data Protection	
<b>2</b>	<b>BROADBAND</b> .....	<b>2</b>
	Connectivity Type, Speed, Resilience	
<b>3</b>	<b>WIRELESS NETWORK</b> .....	<b>3</b>
	Network Performance, Coverage, Management, Security	
<b>4</b>	<b>NETWORK CABLING</b> .....	<b>4</b>
	Copper Cabling, Optical Fibre Cabling, Installation	
<b>5</b>	<b>NETWORK SWITCHING</b> .....	<b>5</b>
	Switch Performance, Management, Security, Resilience	
<b>6</b>	<b>FILTERING AND MONITORING</b> .....	<b>6</b>
	Safeguarding, Management, Monitoring	
<b>7</b>	<b>CLOUD SOLUTION</b> .....	<b>7</b>
	Managing Access, Availability, Data Protection, Backup	
<b>8</b>	<b>SERVERS AND STORAGE</b> .....	<b>8</b>
	Security, Energy Efficiency, Suitable Environments	

# 1 CYBER SECURITY STANDARDS

This standard specifies the minimum requirements for cyber security, user accounts and data protection.

## WHAT ARE THE STANDARDS?

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 standards will protect your school from threats and prepare your school should a cyber security incident happen.

1

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

2

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

3

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

4

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

5

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

6

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

7

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

8

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

9

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

10

Serious cyber attacks should be reported.

11

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

12

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

All standards should be implemented **as soon as possible**.

We are able to guide you through these guidelines and help you implement a cyber security strategy most suitable for your school.

**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.

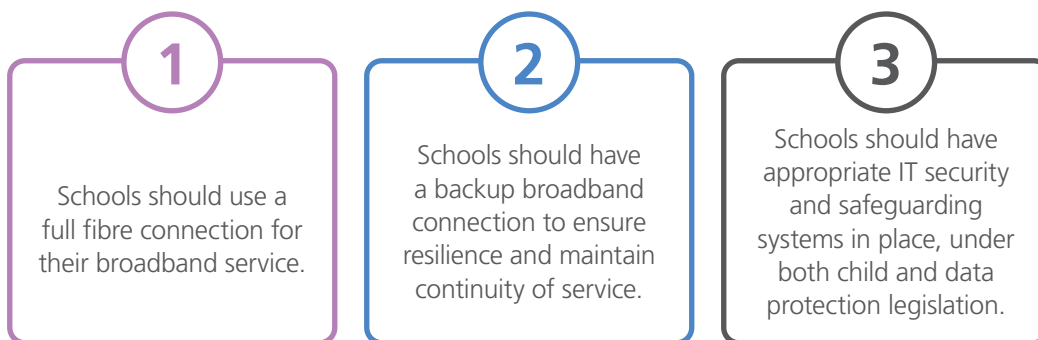


# 2 BROADBAND STANDARDS

This standard specifies the minimum requirements for broadband connectivity type, speed and resilience.

## WHAT ARE THE STANDARDS?

The internet is now an essential service in all schools, new technology means there is now a higher demand for more effective connections. These guidelines emphasise your school needing a full fibre connection alongside a backup broadband and sufficient security and safeguarding processes in place.



### 1. Full Fibre Connection

- This guidance highlights the importance of having a robust connection and infrastructure in place, with full fibre connection (FFTP / Leased Lines) now a necessity.
- It is recommended that you upgrade to Full Fibre Connectivity as soon as possible.

### 2. Backup Broadband

- As the internet is now an essential service in all schools, an automatic failover to an additional backup connection of a different type to your main connection is now required to provide internet continuity. All of our broadband contracts come with the option to include a backup line to ensure resilience and prevent any disruption.

### 3. Security & Safeguarding

Safeguarding your students and staff from potentially harmful and inappropriate material online is essential and your school needs to implement site wide procedures for this. This includes ways to identify, intervene in, and escalate any concerns where appropriate.

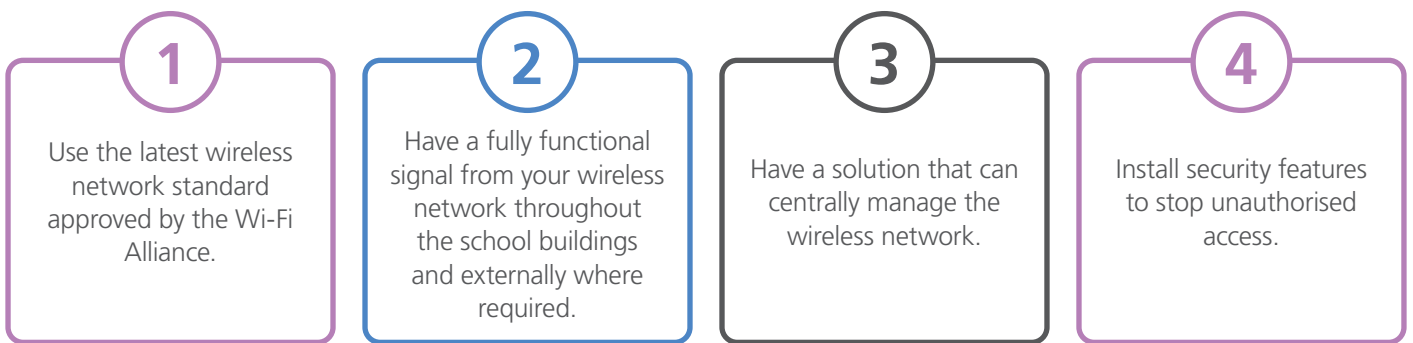
**We can implement a broadband service that will meet these standards, helping you make full use of online resources with a high speed connection you can rely on.**

# 3 Wireless Network Standards

This standard specifies the minimum requirements for wireless network performance, coverage, management and security.

## WHAT ARE THE STANDARDS?

The standards set out four categories the DfE want your school to meet.



### 1. Wi-Fi 6 Standard

Utilising a Wi-Fi Alliance Approved Wi-Fi 6 Standard across your network will provide a high performance solution with the speed and capacity you require to ensure all devices can connect to the network without slowing down operations.

### 2. Fully Functional Network Signal

Your school will need to ensure that there is strong signal coverage across the whole premises where devices are to be used. This means your school requires Wi-Fi Access Points to be introduced across the site.

### 3. Centrally Managed Solutions

As your wireless network will be made up of many access points across the premises, you will require a central management solution where your network can be monitored and configured and issues can be identified and resolved.

### 4. Security Features To Stop Unauthorised Access

Regular and guest users should be set up to prevent unauthorised access, with appropriate authorisation and authentication methods. Any administrative accounts that have access to make configuration changes, must be secure and fully documented.

When your school is ready to upgrade your underperforming and unsupported network, Breathe will be here to help guide you through it.

---

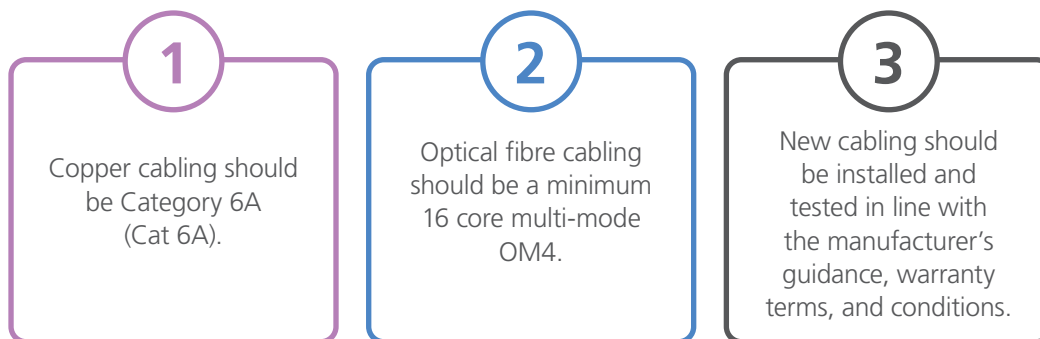


# 4 Network Cabling Standards

This standard specifies the minimum requirements for copper cabling, optical fibre cabling and installation.

## WHAT ARE THE STANDARDS?

Network cabling is the backbone of your network, connecting your infrastructure and devices together. The DfE has issued the minimum standards relating to the specification of your network cabling.



### 1. Category 6a Cabling

This guidance highlights the importance of upgrading to Category 6A cabling. Your school will benefit from greater data capacity than previous copper cabling standards, providing the flexibility to increase the volume and specification of the technology your school requires to connect networks.

### 2. Optical Fibre Cabling

OM4 optical fibre cable has the capacity to transfer data over greater distances and is crucial in ensuring that data is effectively transferred throughout the school. Faulty or inadequate cabling will have a negative impact on network performance quality.

### 3. Cabling Installation

You should meet this standard when you need to replace your current solution that is underperforming as well as in new school builds.

**All new cabling should adhere to the relevant British Standards, which cover network cabling specification, installation, operation, and maintenance.**

We offer network cabling services for upgrades as well as new school builds. We will meet the recommended DfE standards and assist in the design and deployment of network cabling projects for your school.

# 5 Network Switching Standards

This standard specifies the minimum requirements for switch performance, management, security and resilience.

## WHAT ARE THE STANDARDS?

Switches connect network devices and allow them to communicate with one another. The requirements specify four categories in relation to the technical capabilities of your network infrastructure, which the DfE advises your school to meet.

**1**

The network switches should provide fast, reliable and secure connections to all users both wired and wireless.

**2**

Have a platform that can centrally manage the network switching infrastructure.

**3**

The network switches should have security features to protect users and data from unauthorised access.

**4**

Core network switches should be connected to at least one UPS to reduce the impact of outages.

### 1. High-Performance Solution

Schools are high capacity environments, with a large number of users simultaneously accessing the network. A high-performance solution will make sure that the speed and management of data transferred around the network is efficient, secure and doesn't slow down as more devices use it.

### 2. Centrally Managed Solutions

To ensure effective performance, a central management console will enable efficient and secure control and monitoring of the school network.

### 3. Security Features

Network switching infrastructure without adequate security may allow unauthorised users access to secure information, such as student information. You should ensure that switches are configured to support network segregation, security and quality of service.

### 4. Connect To At Least One Ups

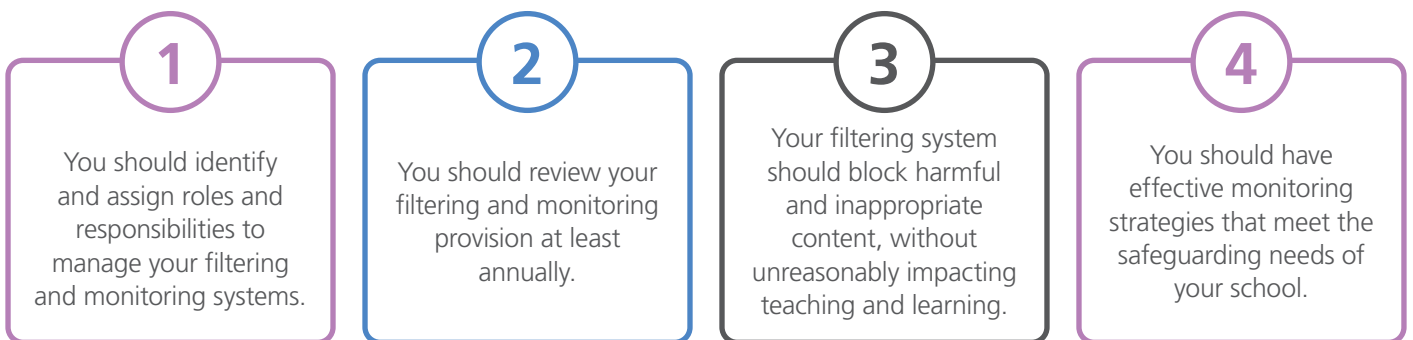
Teaching and administrative operations would be restricted by a total or partial network outage. Therefore, core network switches should be connected to at least one uninterruptible power supply (UPS) to reduce the impact of outages or power surges.

# 6 Filtering And Monitoring Standards

This standard specifies the minimum requirements for filtering and monitoring.

## WHAT ARE THE STANDARDS?

Filtering and monitoring are both important parts of safeguarding students and staff from potentially harmful and inappropriate online material. The following 4 standards have been set out by the DfE to provide a safe environment to learn and work.



### 1. Manage Systems

For effective filtering and monitoring systems to be delivered and maintained, clear roles, responsibilities, and strategies are essential. It's important that the right people are working together and using their professional expertise to make informed decisions.

### 2. Review Annually

You should evaluate your filtering and monitoring provision at least once a year in order to fully understand and evaluate the shifting needs and potential risks of your school.

### 3. Block Harmful Content

An effective filtering system should block internet access to harmful sites and inappropriate content. However, it should not unreasonably impact teaching and learning or restrict students from learning how to assess and manage risk themselves.

### 4. Effective Monitoring Strategy

Monitoring allows you to review user activity on school devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

We can help your school meet the DfE regulations, block unauthorised content and websites and monitor usage.

# 7 Cloud Solutions Standards

This standard specifies the minimum requirements you should meet when using or moving to cloud solutions, including managing access, availability, data protection and backup.

## WHAT ARE THE STANDARDS?

This standard specifies the minimum requirements you should meet when using or moving to cloud solutions, including managing access, availability, data protection and backup.



### 1. Alternative To Locally-Hosted Systems

Utilising cloud solutions lessens the need for local servers and supports your school's overall strategy, lowers costs, enhances business continuity, and boosts security and safety.

### 2. Data Protection

Your school must comply with data protection legislation, with all data handed legally.

### 3. Access Management

You should utilise a central ID and access management tool to fulfil your data protection and safeguarding responsibilities. This will help to secure and safeguard data and increase cyber security.

### 4. Range Of Devices

Cloud solutions should work on a range of devices and be available when needed. This will make it easy for staff and students to work with the data using different systems, from anywhere.

### 5. Backup Provision

The most common risk of cloud data loss is accidental or deliberate data deletion by users. Loss of data can lead to a data breach or prevent critical operations. You must determine the data backup provision you require for each solution in order to comply with this standard.

# 8 Servers and Storage Standards

This standard specifies the minimum requirements for servers and storage, including security, energy efficiency and suitable environments.

## WHAT ARE THE STANDARDS?

The standards set out four categories the DfE want your school to meet. have been set out by the DfE to provide a safe environment to learn and work.

1

All servers and related storage platforms should continue to work if any single component or service fails.

2

Servers and related storage platforms must be secure and follow data protection legislation.

3

All servers and related storage platforms should be energy-efficient and set up to reduce power consumption, while still meeting user needs

4

All server and related storage platforms should be kept and used in an appropriate physical environment.

### 1. Secure And Resilient

Servers and related storage platforms that are designed to be secure and resilient will alert you if a service fails and minimise the risk of systems and data being unavailable. Using cloud solutions reduces the need for local servers.

### 2. Data Protection

All IT systems and services must be 'secure by design' in order to comply with data protection legislation. You need to make sure your servers and related storage platforms are secure and risks are minimised when you buy, install and use them.

### 3. Energy-Efficient


Local servers and their storage platforms run continuously and expend a lot of energy. An energy efficient approach to buying, setting up and using servers and related storage platforms will save energy and money.

### 4. Appropriate Physical Environment

Meeting this standard means servers and related storage platforms should be more secure, have a longer lifespan and be less vulnerable to service failure. Not meeting this standard increases the risk of losing access to critical data and failing to meet data protection legislation.



 [www.breathetechnology.com](http://www.breathetechnology.com)  
*(live chat available)*

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

 [lucy@breathetechnology.com](mailto:lucy@breathetechnology.com)

**breathetechnology**  
support | cloud | security | infrastructure | comms