

breathetechnology

support | cloud | security | infrastructure | comms

EMPOWERING EDUCATION THROUGH SECURE TECHNOLOGY

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



SONICWALL SHOP
A Breathe Technology Business

DfE School Guidance – **Meeting Cloud Solution Standards**

Is your school meeting the DfE's Cloud Solution Standards?

In January 2024, the Department for Education updated their guidance to schools regarding how to meet digital and technology 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.

Cloud solutions or services are hosted and managed on the internet rather than locally in the school. They can be accessed from a wide range of devices at anytime from anywhere with an internet connection.

The DfE's Cloud solution Standards set out five categories your school needs to meet:

- Use cloud solutions as an alternative to locally-hosted systems, including servers.
- Cloud solutions must follow data protection legislation.
- Cloud solutions should use ID and access management tools.
- Cloud solutions should work on a range of devices and be available when needed.
- Make sure that appropriate data backup provision is in place.

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 fulfil these requirements.

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



1 Alternative to locally hosted systems

Utilising cloud solutions lessens the need for local servers, supports your school's overall strategy, lowers costs, enhances business continuity, and boosts security and safety. The more cloud solutions you use, the more your school will benefit in the areas described in this standard.

Use cloud solutions as an alternative to locally-hosted systems and servers

The importance of meeting the standard

Using cloud solutions reduces the need for local servers. This can:

- support your overall school strategy
- allow you to take advantage of low-cost or free cloud services for some applications
- save money by reducing on-site equipment and energy costs, as well as the need for support and licensing
- improve safety and security by increasing resilience to cyber attacks
- improve reliability and business continuity

It can also save time by:

- allowing users to work more flexibly and collaboratively
- outsourcing hardware and software updating and maintenance

Many schools are using a hybrid model, with some cloud solutions running alongside those on on-site servers. The more cloud solutions you use, the more your school will benefit in the areas as described in this standard.

Local servers may still be needed for some systems, such as access control (door security), building management, or cashless catering.

How to meet the standard

Before moving to the cloud:

- understand the software, devices and data you currently use and what you use them for
- consider the types of data you need to import and export easily from the cloud
- ask your IT service provider about free cloud services your school can benefit from

Use this information to assess where you can replace servers with cloud solutions. This should include assessing files, documents and shared folders.

Ask your IT service provider to set up your cloud solutions to meet the standards described in the technical requirements of this standard. Your IT service provider may be a staff technician or an external service provider.

Training users to use your cloud solutions will make sure that they are confident in using the solutions correctly. This will help your school to realise the benefits listed in this standard.

Free training and refresher training options may be available online. Your cloud solution provider may also be able to provide system specific training and support.

Technical requirements to meet the standard

Cloud solutions need a level of security to be in place to make sure data is used, stored and transferred safely. You should do this by following the cyber security standards for schools and colleges.

To make sure cloud solutions can be used effectively you must have reliable broadband with

the capacity to support your needs. You should do this by following the broadband internet standards for schools and colleges.

Cloud solution performance will depend on your network capacity, reliability and availability. Check that you meet the following:

- network switching standards for schools and colleges
- network cabling standards for schools and colleges
- wireless network standards for schools and colleges

Ask your IT service provider to make sure that data used in the cloud solution is portable and it allows for:

- secure encrypted transfer
- data export to an open standard or commonly used format (for example, spreadsheet or tabular data should be exportable as .CSV and/or .ODT files)
- data links through secure, documented application programming interfaces (APIs)
- a timely process for data transfer in an open standard or neutral format if you end the contract

2 Data Protection

Your school must comply with data protection legislation, with all data handed legally. If you are storing or processing sensitive personal data, you might need extra security measures to make sure you meet statutory data protection and UK GDPR requirements.

Cloud solutions must follow data protection legislation

The importance of meeting the standard

You must comply with data protection legislation.

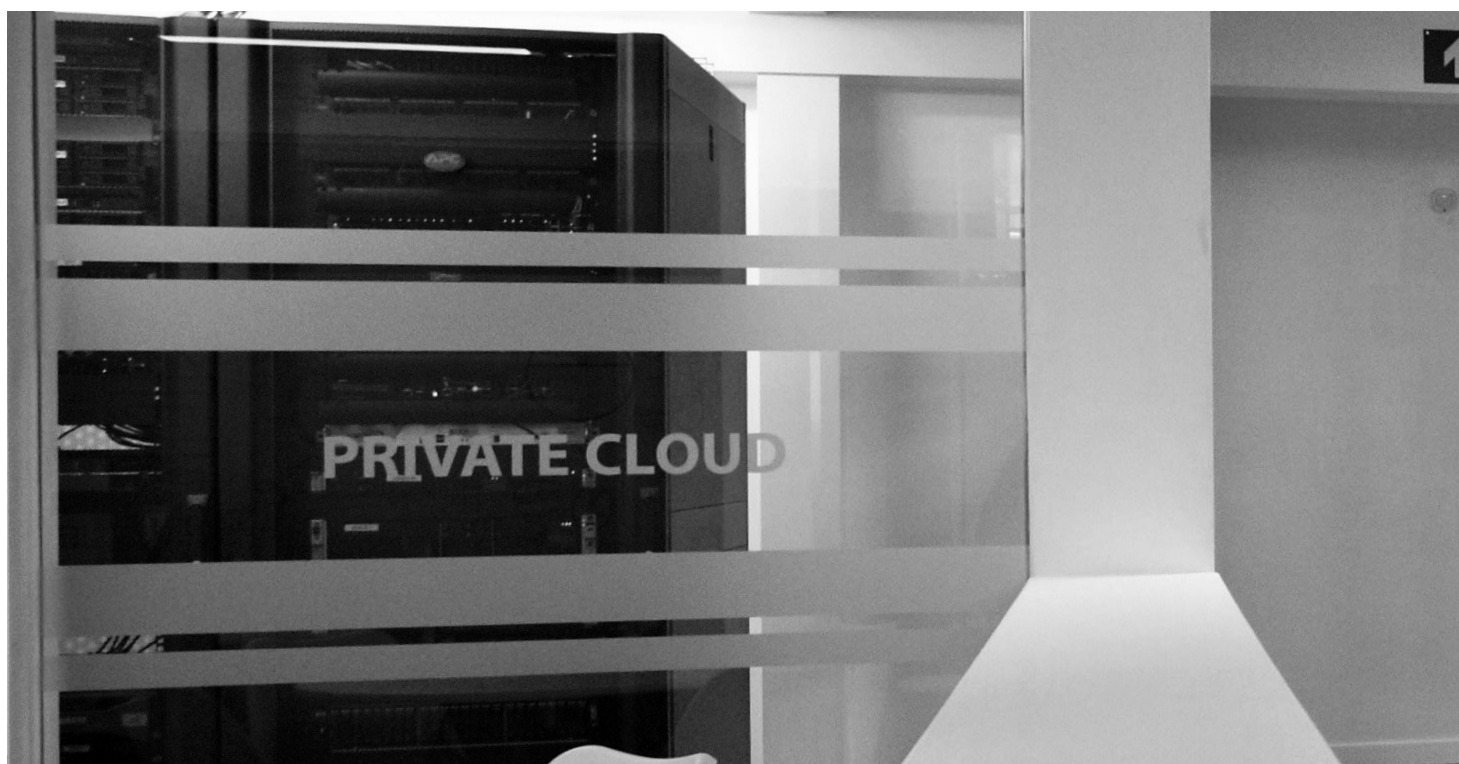
How to meet the standard

Responsible bodies must seek assurance from cloud solution and IT service providers that data is being handled legally.

Ask your IT service provider to set up your cloud solutions to meet the following standards described in the technical requirements.

Your IT service provider should consult with your data protection officer (DPO) on data protection issues such as data retention and sharing.

Your IT service provider may be a staff technician and or an external service provider.



Technical requirements to meet the standard

Your DPO should carry out data protection impact assessments (DPIA) for any cloud solutions that store personal and or sensitive personal data (also known as special category data).

This example of how to record your DPIA process and outcome might be useful.

Check whether the data you want to store and process in the cloud is personal and or sensitive personal data.

If you are storing or processing personal and or sensitive personal data, you might need extra security measures to make sure you meet statutory data protection and UK GDPR requirements. This might include measures such as encryption, password protection, or more restricted access.

All systems need to follow the National Cyber Security Centre (NCSC) cloud security principles. Make sure:

- data processing carried out by third parties is covered by an appropriate contract
- there is a user account creation, approval and removal process that is part of your school's joining and leaving protocols, and it complies with data protection legislation
- there is a data sharing agreement with your cloud solution provider
- roles and responsibilities for dealing with a data breach are clearly documented

Your data sharing agreement needs to state that the cloud solution provider will share information promptly if there is a data breach. This lets the data controller take the necessary actions.

Data should be stored and processed in the UK or EU, unless you have confirmed that any international transfer of your data complies with UK GDPR. See the Information Commissioner's Office guidance on how to make a restricted transfer in accordance with the UK GDPR for more information. Ask your provider about this.

3 Access Management

Many cloud solutions work independently from each other and need multiple logins and passwords. Therefore, 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 by providing one centrally managed account.

Cloud solutions should use ID and access management tools

The importance of meeting the standard

- Many cloud solutions work independently from each other and need multiple logins and passwords. To meet your data protection and safeguarding obligations, you should use a central ID and access management tool. This will help to secure and safeguard data and increase cyber security by:
- providing one centrally managed account with one log in for each user so that users don't need to remember multiple passwords
- simplifying login organisation and management when users join or leave
- managing access to systems based on groups so that the right people get access to the right tools

How to meet the standard

Ask your IT service provider to set up your cloud solutions to meet the standards described in the technical requirements.

Your IT service provider may be a staff technician and or an external service provider.

Make sure:

- your IT service provider assesses your existing or potential cloud solutions and work with them to choose an appropriate ID management system
- the system is used to secure all current and future cloud solutions and systems (including curriculum tools)

The DfE's get help buying for schools service can help you to buy ID management tools.

Technical requirements to meet the standard

To meet this standard you should:

- test it with all systems and make sure this is the only way staff and students can log on
 - have agreed, documented processes in place to manage the addition and removal of users
 - create roles that make sure all types of users have the right levels of access to the right systems
 - make sure that your IT service provider has separate, secure access to your cloud solution, independent of the ID management system
-

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. Poor or unreliable availability of a cloud solution could have a significant impact on running your school.

Cloud solutions should work on a range of devices and be available when needed

The importance of meeting the standard

Good access and availability will make it easy for users to work with the data using different systems, from anywhere and from a range of devices.

Poor or unreliable availability of a cloud solution could have a significant impact on running your school or college.

How to meet the standard

Before entering a cloud solutions agreement, make sure you understand how and when it will need to be accessed by users.

When procuring cloud solutions make sure published availability targets meet your needs. You should trial the cloud solutions before committing to buy to make sure performance meets expectations.

Availability targets provided by cloud suppliers may appear misleading. Cloud solutions run 24 hours a day and 7 days a week. This means that less than 1% difference in cloud availability can significantly affect downtime and performance. The following percentages translate to the downtime shown:

- 99% availability = approximately 7 hours of downtime per month
- 99.9% availability = approximately 45 minutes of downtime per month
- 99.99% availability = approximately 5 minutes of downtime per month

Work with your IT service provider during procurement to make sure the technical requirements are met.

Your IT service provider may be a staff technician or an external service provider.

Technical requirements to meet the standard

To meet this standard you should:

- make sure that you can easily access data from the cloud solution in a way which meets your and your users' needs
- allow easy but secure access from a range of devices, ask your cloud provider about secure access to their services

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

Make sure that appropriate data backup provision is in place

The importance of meeting the standard

The most common risk of cloud data loss is accidental or deliberate data deletion by users. Although data loss by cloud providers is uncommon, it can happen.

Loss of data can lead to a data breach and mean you need to inform the appropriate authorities. It may also obstruct or prevent critical business operations.

Cloud providers will only hold backup data for a limited period. This could be for as little as 30 days with some providers. This will depend on your service level agreement.

Your data protection officer (DPO) should know which data is critical. They will also know how long different types of data should be kept for.

For more information, refer to the National Cyber Security Centre (NCSC) backup guidance.

How to meet the standard

Working with your DPO and IT service provider, make sure you understand your cloud provider's backup processes and policies. Ask:

- what data do they backup?
- where is it held (for UK GDPR compliance)?
- how long is the data held for?
- how frequently are backups made?

Ask your IT service provider to set up your cloud solutions to meet the standards described in the technical requirements.

Your IT service provider may be a staff technician or an external service provider.

Technical requirements to meet the standard

To meet this standard you should identify the data backup provision you need for each solution. This should be based on the data it will store. Consider:

- its sensitivity
- its importance to normal operations
- the impact if it were to be unavailable temporarily or permanently
- how long you could be without the data before it becomes an issue
- balancing cost against need, frequent backups are more expensive so consider the cost against the age of the data you recover from a backup
- for critical data use the 3-2-1 rule, at least 3 copies, on 2 devices and 1 offsite

Third party solutions and plug-ins are available for cloud solutions that do not meet your data backup needs. You should discuss this with your cloud solution provider.



When should you meet the standards?

For data protection and backup provision, your school should already be meeting these standards to help safeguard, protect, and secure your data and systems, as well as meet data protection legislation. You should be upgrading from locally hosted systems as well as using an access management tool as soon as possible to realise the benefits. You should meet the cloud availability standard for existing and new cloud solutions.

You should be upgrading from locally hosted systems as well as using an access management tool as soon as possible to realise the benefits.

You should meet the cloud availability standard for existing and new cloud solutions.

What we can do to help you

Breathe delivers scalable, on-demand cloud solutions for schools, custom-tailored to meet your needs. From revamping telephony systems to robust cloud servers and storage, we provide a full suite of flexible, secure, and efficient solutions, ensuring you not only meet but exceed industry standards.

From our MD Breathe Technology



Craig van Aswegen – MD & Chartered IT Management Consultant

“As an IT management and cyber security consultant who spends most of my time with academy trusts and schools, I understand the challenges involved in managing IT in today’s world. Especially not losing sight of who our true stakeholders are in schools.

I.T. is a supporting function that enables and empowers teaching and learning as its main goal. Digital transformation is critically important, but there are some real challenges when working with schools on their IT strategy and cyber security.

When working with MAT’s, there is additional complexity as we’re starting to talk about the benefits that schools should get from centralised services and being part of the bigger organisation with its enterprise level of IT.

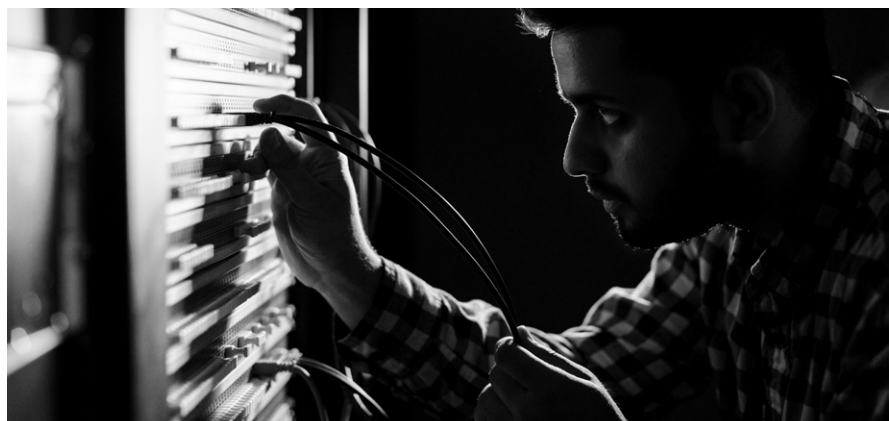
Apart from the financial burdens, it’s not always easy to ensure that we

meet the latest DfE guidelines for technology or even keep on top of the government guidelines around cyber security and backup.

We often start the process with an IT or cyber security audit because it allows you to first understand what is in place. Review the facts, highlight the issues and risks, and then provide viable suggestions and recommendations.

Taking into account our extensive experience, the DfE, KCSIE, and national cyber security guidelines, amongst other industry body advice and best practices.

Ultimately, we simplify it for our schools. We work best alongside the SLT and as an extension of the internal IT team, helping them to achieve the next level in school IT. This is what we are good at, passionate about, and the reason Breathe exists.”






At Breathe, we provide scalable on-demand cloud solutions to help schools on their cloud journey.

We offer a range of cloud services tailored to your school's needs and proactively support you to ensure the quality and reliability of our services, ensuring that you are not only meeting, but excelling these standards.

From a complete overhaul of your telephony systems to powerful cloud servers and storage for your school, we can offer a full suite of cloud solutions with the flexibility, security and efficiency you require.

 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