Department for Education

Title:	**Cloud Solution Standards**
Published:	29 03 2023
Updated:	--

Find out what standards your school or college should meet on cyber security, user accounts and data protection.

Prepared from information from the DfE by the Association of Network Managers in Education.
www.anme.co.uk

Standard 1

Using cloud solutions as an alternative to locally-hosted systems, including 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 onsite equipment and energy costs, and 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 onsite 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

Dependencies to the standard

As well as the standards highlighted in the technical requirements, check that you meet all the cloud solution standards.

When to meet the standard

You should meet this standard as soon as possible to realise the benefits.

Standard 2

Cloud solutions must follow data protection guidelines

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 standards described in the technical requirements below.

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.

The DfE data protection in schools toolkit gives general data protection advice and guidance that may help you to meet this standard.

Dependencies to the standard

Check that you meet the cyber security standards for schools and colleges.

When to meet the standard

You should already be meeting this standard in accordance with data protection legislation. For more information see the data protection in schools toolkit.

Standard 3

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

Dependencies to the standard

Check that you meet the cyber security standards for schools and colleges.

When to meet the standard

You should meet this standard as soon as you can. It helps to keep your data and systems secure.

Standard 4

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

Dependencies to the standard

Check that you meet the cyber standards for schools and colleges.

When to meet the standard

You should meet this standard for existing and new cloud solutions. This will help to make sure that data is available and accessible to all users when it is needed.

Standard 5

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?

For more information, refer to the NCSC cloud security principles.

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.

Dependencies to the standard

Check that you meet the servers and storage standards for schools and colleges.

When to meet the standard

You should already be meeting this standard to help safeguard, protect and secure your data and systems. It is also a requirement for meeting data protection legislation.