Department for Education

Title:	**Servers and Storage Standards**
Published:	29 03 2023
Updated:	--

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

Standard 1

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

The importance of meeting the standard

Servers and related storage platforms designed to be secure and resilient will:

- be more reliable
- make sure your IT support provider can monitor performance and alert you if a component or service fails
- minimise the risk of systems and data being unavailable

Not meeting this standard could lead to:

- a loss of data
- difficulties running your school or college
- an increased risk of a cyber attack or incident
- your school or college temporarily closing

How to meet the standard

Using cloud solutions reduces the need for local servers. Reading the cloud standards for schools and colleges with your IT service provider will help you to assess where you can replace or reduce server resources.

Ask your IT service provider to set up your servers and related storage platforms to meet the technical requirements of this standard.

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

Technical requirements to meet the standard

Review your existing servers and related storage platforms regularly with your IT service provider to make sure that they are fully resilient.

Your senior leadership team will need to decide the maximum downtime it is willing to accept. This should be based on your specific needs, including the:

- sensitivity of the system and data
- importance of the system and data to running your school or college

For all servers make sure that you have:

- asked your IT support provider to monitor performance and alert you if a

component or service fails

- processes to replace any failing or failed components quickly
- valid manufacturer warranties and support agreements
- a process to make sure that patches and firmware upgrades are up to date and managed in line with manufacturer recommendations
- a process to replace servers and related storage platforms when they're approaching end of warranty, end of support, or end of life

Servers containing critical data should have at least the following:

- multiple power supplies for servers which switch seamlessly if the power fails
- an uninterruptible power supply (UPS) with automatic, safe shutdown of servers and a minimum of 30 minutes run-time
- a hard disk set up with mirroring (which duplicates data in real time), redundancy (which allows a server to continue to operate normally if one disk fails), or both
- a regular backup of the systems and data
- backup servers (onsite or in the cloud) and network cards that switch over seamlessly when one fails
- valid manufacturer warranties and support agreements, with service levels matched to how critical the data is

For anything not covered by the manufacturer warranties, consider keeping spare components for items most likely to fail. For example, spare fans, power supplies and disks.

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 to help safeguard, protect and secure your data and systems. It is also a requirement for meeting data protection legislation.

For more information see the data protection in schools toolkit.

Standard 2

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

The importance of meeting the standard

To meet data protection legislation all IT systems and services must be ‘secure by design’.

You need to make sure your servers and related storage platforms are secure and risks are minimised when you buy, install and use them. This makes sure that systems and data are safe from any potential risks of damage or data loss. This could include:

- physical damage to the server such as flooding or fire
- virtual damage caused by a cyber attack or incident
- human error through poor management

How to meet the standard

Ask your IT service provider to set up new and existing devices to meet the technical requirements of this standard.

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 or an external service provider.

When buying any new systems or services, you should make sure systems and services are secure. School business professionals and the IT service provider should work together to choose suppliers on the basis of their ability to meet the technical requirements described in this standard.

You can use the get help buying for schools service for free help and support with buying ICT goods and services.

Technical requirements to meet the standard

To meet this standard your IT provider must:

- meet the cyber security standards for schools and colleges
- make sure that your servers and related storage platforms are secure, licensed, updated and well-managed
- review your existing systems and services whenever you make a change or at least each term, to make sure that they are secure

Your DPO should carry out data protection impact assessments (DPIA) for any server and related storage 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 server and related storage platforms 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) 10 Steps to Cyber Security guidelines.

Make sure:

- 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
- roles and responsibilities for dealing with a data breach are clearly documented

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 to comply with data protection legislation.

Standard 3

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

The importance of meeting the standard

Local servers and their storage platforms run continuously. This means they can use a lot of energy.

An energy efficient approach to buying, setting up and using servers and related storage platforms will save energy and money.

How to meet the standard

School business professionals and the IT service provider should work together to make sure:

- energy efficiency is a stated requirement in all server and related storage platform procurements
- the existing server and related storage platforms are set for the highest level of energy efficiency while still meeting user needs for speed and ease of use

Ask your IT service provider to meet the technical requirements of this standard.

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

Using cloud solutions increases your overall energy efficiency. Reading the cloud standards for schools and colleges with your IT service provider will help you to assess where you can replace or reduce server resources.

Technical requirements to meet the standard

Make sure your servers and related storage platforms are energy efficient by:

- using power saving when they're inactive, as long as this does not significantly reduce server performance, prevent backups, or risk damage to the equipment
- turning off any features which are not used

When buying servers and related storage platforms make sure you:

- specify servers that are designed to be energy efficient, with the ENERGY STAR label or equivalent
- include a requirement that all server and related storage platforms are set up to reduce energy consumption as much as possible
- are meeting your immediate needs and plans for growth, but do not go beyond that
- are getting a solution that is durable, easy to maintain and repairable

When to meet the standard

You should review your existing servers and related storage platforms now to make sure they meet the standards.

You should continue to meet these standards if you buy any new servers and related storage platforms.

Standard 4

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

The importance of meeting the standard

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
- the servers or related storage platforms not working
- failing to meet data protection legislation

How to meet the standard

Using cloud solutions reduces the need for local servers. Reading the cloud standards for schools and colleges with your IT service provider will help you to assess where you can replace or reduce server resources.

Make sure that your servers and related storage platforms can only be accessed by people who have a genuine need to do so.

Ask your IT service provider to set up your servers and related storage platforms to meet the technical requirements of this standard.

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

Technical requirements to meet the standard

Make sure servers are in a dedicated, secure, locked room or cupboard that is not used for other purposes.

The room should meet the size requirements set by the Health and Safety Executive and British Standards. The required size for a server room is:

- depth (for a 1000mm deep cabinet): 3.4m
- width (for an 800mm wide cabinet): 2.2m

For each additional server cabinet, use the same minimum depth and increase the width by 0.8m, leaving 1.4m to the side wall (as set out in BS EN 50174-2 of the installation planning and practices inside buildings).

The room or cupboard should also:

- have servers mounted or stored in cabinets
- be free of flammable items, such as paper, boxes, clothing, solvents or chemicals
- have a dedicated power supply that can meet or exceed current demand (this must be an isolated uninterruptible supply, to prevent server or storage outages for key equipment)
- have sufficient cooling or mechanically assisted ventilation to keep server equipment within manufacturers' recommended temperature guidelines

The room can not:

- contain battery-powered end user devices, such as laptops, due to a potential fire risk
- have any windows or be accessible directly from a classroom
- store any liquids in it, such as bottles or water or hot drinks

Other potential threats you need to prevent include:

- leaking pipework for water, heating, drainage, or vents
- water sources in rooms above (for example, toilets or science labs)
- equipment such as water tanks, heating equipment or boilers
- dust from building work

Dependencies to the standard

Check that you meet:

- cyber security standards for schools and colleges
- network cabling 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.

For more information see the data protection in schools toolkit.