Department for Education

Title:	**Laptop, desktop, and tablet standards**
Published:	16 01 2024
Updated:	--

Find out what standards your school or college should meet on laptops, desktops and tablets.

Having the right devices for students and staff will help support the digital technology strategy of the school or college.

Throughout these standards we refer to:

- laptop, desktops and tablets as devices
- the person in the senior leadership team (SLT) who is responsible for digital technology as the SLT digital lead (for more information on this role see our digital leadership and governance standards)
- in-house or third-party support as IT support

The job titles in these standards may not fit in a school or college's educational setting, but the responsibilities described should be applied to the most relevant person.

You can also see more details on how to use the standards to help your school or college meet their digital technology needs.

Standard 1

Devices should meet educational needs and support the digital technology strategy

Why this standard is important

Providing devices that meet educational needs and support the digital technology strategy will help:

- curriculum planning and delivery
- administration, including data and financial management
- flexible and cross-site working

Devices that are not suitable may:

- lead to lost learning or disrupt day to day operations
- not be safe and secure
- need to be repaired and replaced more often
- cost more in the long run

Who needs to be involved

The senior leadership team (SLT) digital lead should work with:

- other SLT members to make sure any decisions on devices fits with the school or college's digital technology strategy
- IT support to assess if devices meet the needs of students and staff, and identify any additional technical requirements

How to meet this standard

To meet this standard, the SLT should follow this 3-step process to understand which devices are needed.

1. **Create a digital strategy**

   For more details, see our standards on digital leadership and governance.

2. **Identify the device needs of students and staff**

   The SLT digital lead should assess how devices will support the needs of students and staff, based on the school or college's digital technology strategy.

They should look at how devices are being used, including who uses them, where they are being kept and what they are being used for. This will help them identify:

- the number and type of devices needed
- any specific physical requirements for devices
- the level of technical support needed
- training requirements for students and staff

3. **Assess the security and technical requirements of the devices**

   The SLT digital lead should work with IT support to assess the security and technical requirements of devices. This will help determine whether they need to buy new devices or if they can repurpose existing ones.

When to meet this standard

This standard should be met when the SLT review the use of laptops, desktops and tablets, or buy new devices.

Related standards

The following standards should also be considered when reviewing your use of laptops, desktops and tablets:

- cyber security
- filtering and monitoring
- cloud solutions
- wireless network
- broadband internet

Standard 2

Devices should be safe and secure

Why this standard is important

Keeping devices safe and secure will protect those who use them, the network and the data on them. This will:

- make it easier to apply security and safeguarding policies to each device
- minimise the risk of cyber security incidents and data breaches

The risks of not doing this include:

- students accessing harmful or inappropriate material
- lost learning due to cyber incidents or data breaches
- difficulty managing safeguarding
- loss of public confidence and reputational damage

Who needs to be involved

To meet this standard, the SLT digital lead should make sure all devices are centrally managed and meet the needs of those using them.

IT support should check all devices are configured securely. They should also work with the designated safeguarding lead to review the filtering and monitoring requirements of the devices.

The data protection officer should also be involved, when reviewing data security.

How to meet this standard

To meet this standard, the SLT digital lead should protect all devices against the risk of data breaches, and cyber security and safeguarding incidents.

To do this, IT support should work with the designated safeguarding lead to check and confirm all devices meet the Keeping children safe in education (KCSIE) requirements for:

- information security and access management
- filtering and monitoring

All new devices must be compatible with existing filtering, monitoring and security systems.

If any existing devices are not compatible with existing filtering, monitoring and security systems, you should look to alternative solutions before using the device.

Filtering and monitoring, and cyber security for all devices must be reviewed regularly.

For more details see the standard topics:

- Filtering and monitoring standards for schools and colleges
- Cyber security standards for schools and colleges

Configuring devices securely

IT support should also check all devices are configured securely:

- with a protective firewall on the network or device
- by using virtual area local networks (VLANs) which add separate layers of protection on the network between different types of devices and users
- with managed anti-virus and anti-malware software
- with enterprise or education-grade operating systems, including support and up-to-date security patches
- with labels or tags to keep track of them when you buy them and add them in an asset register
- with accessibility features that are not blocked by security policies

For further support, the National Cyber Security Centre (NCSC) has published guidance on how to choose, configure, and use devices securely.

Centrally managing devices for greater security

Devices should be centrally managed by IT support. This includes:

- making sure security and safeguarding policies are applied consistently
- updating and applying security patches to software and applications
- recording up-to-date information about the device in the asset register
- restricting and monitoring access to browsers by making changes to the technical policies and settings set on core systems

Mobile and portable devices should have mobile device management to minimise safeguarding and security risks. This means IT support can remotely manage devices, including:

- locking or wiping them
- securing apps and software

Carrying out a data protection impact assessment

The data protection officer should support the creation of a data protection impact assessment (DPIA) for all existing devices and whenever new ones are bought. This assesses the risk:

- to personal or sensitive data
- of taking school or college owned devices offsite
- of bring your own device strategies, making sure they comply with security and safeguarding requirements

When to meet the standard

This standard should be met now for all laptops, desktops and tablets currently used.

Related standards

When disposing of devices, see the standard in this topic, 'Make sure devices are energy efficient, and they are bought and disposed of sustainably'.

The following standard topics should also be considered when reviewing the safety and security of your devices:

- cloud solutions
- wireless network
- broadband internet
- digital leadership and governance

Standard 3

Devices should meet or exceed the minimum requirements

Devices should be assessed against the needs of students and staff. All devices should also meet or exceed the minimum requirements set out in this standard.

This will make sure devices are:

- safe and secure
- stable and reliable

Not meeting these requirements could mean your devices:

- negatively impact teaching and learning
- are at risk of malware, ransomware and potential data breaches
- are not value for money

IT support should work with the SLT digital lead to make sure all devices meet the requirements in this standard.

How to meet the standard

IT support should review the minimum requirements set out in this standard.

Devices should also be reviewed once a year to take account of any changes to the minimum requirements set out in this standard.

Minimum Requirements

The purpose of the requirements in this section is to make sure schools and colleges have reliable and durable devices which support curriculum delivery.

This is not a fully inclusive list for all device requirements, as these will depend on specific needs.

IT support should make sure all devices meet or exceed the minimum requirements set out in this table.

Minimum requirements	What you need
Operating system	Enterprise or education-grade operating systems, which means they are designed for professional rather than home use.
Support and security	When repurposing, upgrading or buying new devices tablets should have 3 years of manufacturer support and security patches. Laptops and desktops should have 5 years of support and security patches.
Warranty length	3 years for laptops and desktops 2 years for tablets The warranty durations listed here have been set to cover the minimum amount of time manufacturers usually offer support for security updates and bug fixes.
Wirelessly connecting to the IT network (for portable devices)	Devices should support the wifi standard 802.11ac Wave 2. But it's recommended that devices meet wifi 6 (802.11ax).
Screen size (for tablets only)	9.7 inches

When to meet the standard

Laptops, desktops and tablets should be replaced or upgraded now if they do not meet the operating system requirements of this standard.

For everything else:

- check whether they can be upgraded or repurposed before choosing to buy any new devices
- make sure this standard is met when investing in new devices

Related standards

The following standard topics should also be considered when reviewing device requirements:

- filtering and monitoring
- cyber security
- cloud solutions
- wireless network
- broadband internet
- leadership and governance standards

Standard 4

Make sure devices are energy efficient, and they are bought and disposed of sustainably

Why this standard is important

Devices can be one of the biggest sources of energy use in schools and colleges. Taking an energy efficient approach to the buying, setting up, using and disposal of devices will help with cost savings and sustainability.

If this standard is not met, there is a risk of:

- increased costs by using more energy than you need
- creating unnecessary waste
- it negatively impacting the environment

Who needs to be involved

To meet this standard the senior leadership team (SLT) digital lead should work with:

- the school, college and trust business professionals
- IT support

How to meet this standard

The SLT digital lead should review the use of both existing and new devices.

For existing devices make sure they:

- are switched off when not in use
- automatically power off when they do not need to be used out of hours
- are only using the tools needed

When buying new devices check whether:

- existing ones can be repurposed
- they are rated with a low energy certification, such as Energy Star

When disposing of devices, IT support should make sure that:

- Waste Electrical and Electronic Equipment (WEEE) regulations and data protection requirements are met
- they have certificates for WEEE, disposal and destruction of data
- the IT asset register is updated
- action is taken to prevent security incidents by removing or destroying any data on the devices

For more information refer to the National Cyber Security Centre's (NCSC) guide to the secure sanitisation of security media.

When to meet this standard

The WEEE regulations are a legal requirement. The SLT should consider energy efficiency the next time they invest in new devices. They should also review how existing devices are used, as set out in this standard.

Related standards

The following standard topics should also be considered when reviewing device requirements:

- cyber security
- cloud solutions

For more details on asset registers visit the digital leadership and governance standard, 'Keep registers relating to hardware and systems up to date'.