Department for Education

Title:	**Digital Leadership and Governance Standards**
Published:	16 01 2024
Updated:	--

Find out what standards your school or college should meet on digital leadership and governance.

Good digital technology governance:

- identifies roles and responsibilities
- establishes critical processes to manage digital technology
- ensures that up-to-date information on the school or college’s digital technology is available to support decision making

We refer to hardware, software and digital services as digital technology throughout the following standards.

The job titles in these standards may not fit in your educational setting, but the responsibilities described should be applied to the most relevant person.

You should complete the first 3 standards before moving to the last standard on creating your digital technology strategy. This is so you can successfully build your strategy in line with your school or college’s development plan.

Visit our standards page for more details on how to use the standards to help your school or college meet their digital technology needs.

Standard 1

Assign a senior leadership team (SLT) member to be responsible for digital technology

Why this standard is important

Schools and colleges need a member of their SLT to:

- have strategic oversight of all digital technology and how it fits with their development plan
- create and manage the digital technology strategy led by the needs of staff and students, not the technology itself
- help all staff to embed digital technology that meets staff and student needs

Having clearly defined roles and responsibilities will help schools and colleges focus the digital technology strategy around their development plan. Without this focus, there's a risk that:

- the use of technology will only meet short-term needs that could potentially lead to additional unplanned costs
- schools and colleges will be exposed to safeguarding and security issues
- new digital technology will not be compatible with existing technology used by the school or college

Who needs to be involved

The headteacher or principal will have responsibility for making sure this standard is met by assigning a SLT digital lead.

The SLT digital lead is usually someone with teaching experience. They will act as a link between:

- technical staff
- the SLT
- curriculum leads
- the data protection officer
- the designated safeguarding lead
- school, college and trust business professionals or the finance team
- the trust IT director or equivalent (if applicable) to align with the digital technology strategy

How to meet this standard

To meet this standard you must:

To meet this standard, the headteacher or principal should appoint someone who is responsible for digital technology. They do not need to be an expert, but some technical knowledge or interest could be advantageous for this role.

They will be accountable for:

- the delivery of the digital technology strategy based on teaching and learning outcomes and organisational needs
- encouraging and supporting the use of digital technology across the school or college
- reviewing the effectiveness of IT support to inform decision making and taking action, when necessary
- identifying and acting on digital technology training needs for staff and students

Governors or trustees should also consider assigning a digital link role within the governing body or board of trustees.

When to meet the standard

You will need to assign the role of the SLT digital lead within your school or college before you can create your digital technology strategy.

Standard 2

Keep registers relating to hardware and systems up to date

Why this standard is important

A contracts register, asset register and information asset register will help your school or college to:

- understand what digital data, equipment and systems you have
- manage digital data, equipment and systems effectively
- keep track of buying and licensing so that schools or colleges can get better value for money when renewing software and hardware

Not having these registers in place for digital technology could lead to:

- budget pressures due to accidental renewal of subscriptions, software and hardware that might not be needed, or are not the best value for money
- safeguarding and cyber security issues as software might not be up to date
- lost learning and workload burdens if software or hardware is not budgeted for or supported

Who needs to be involved

To meet this standard, the senior leadership team (SLT) digital lead will need to work with the following people:

- school, college or trust business professionals or the finance team
- the data protection officer
- IT support

How to meet this standard

To meet this standard, schools and colleges should include digital technology within their:

- contracts register
- asset register
- information asset register

By including digital technology in these documents, schools and colleges will know what contracts, digital technology and data they have, and when they need to be reviewed.

Contracts Register

The contracts register includes, but is not limited to:

- licenses
- subscriptions
- contracts related to your broadband, IT support and technology provider
- a list of your school or college’s approved apps

It can also capture the value of the contracts which helps to monitor spend and make savings where possible.

Commercial and procurement information should be updated by the business or finance team, and IT support should update technical information. This contract register must be kept up to date.

Asset Register

An asset register is a log of all the physical digital technology and tools that are within the school or college and should detail:

- what equipment you have
- asset numbers
- serial numbers
- who it is assigned to
- where it is within the school or college
- when it was purchased
- how old it is – this may be different to how long you have owned it, as it may be second-hand equipment
- when it is due for review so that you can consider a replacement or upgrade
- date it was securely disposed of

The SLT digital lead owns this register and is responsible for making sure processes are in place for IT support to keep the register up to date.

Information Asset Register (IAR)

An IAR is a log of the digital data that is held on staff and students and is owned by the data protection officer. The SLT digital lead is responsible for making sure there is a process in place for:

- IT support to update the data protection officer on any digital technology data that needs to be included in the register
- the data protection officer to use the existing IAR to identify and report any potential changes that may need to be made to your digital technology strategy to the SLT digital lead – for example, if your IAR identified the need for security improvements with your servers
- reviewing the digital technology aspects of the IAR

When to meet the standard

You should already be updating your registers every time something changes.

However, the SLT digital lead should review these registers ahead of your next financial planning cycle, and before you move on to the next standard to create your digital technology strategy.

Related Standards

The following standards should also be considered when documenting and monitoring your data, equipment, and systems.

Servers and storage standards

- Servers and related storage platforms must be secure and follow data protection legislation
- All server and related storage platforms should be kept and used in an appropriate physical environment

Cyber security standards

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

Laptops, desktops, and tablets standards

- Devices should meet educational needs and support the digital technology strategy
- Make sure devices are energy efficient, and they are bought and disposed of sustainably

Standard 3

Include digital technology within disaster recover and business continuity plans

Why this standard is important

You should have a process in place to review and update the disaster recovery and business continuity plans, including those related to digital technology.

Not doing so will risk:

- significant disruption to a school or college in the event of a disaster, such as a cyber attack
- unplanned spend from a disaster that was not expected
- potential loss of data or a data breach

This process will help your school or college to continue to operate and provide teaching and learning even during emergencies. This will help prevent lost learning and will also mean that:

- staff, students and parents or carers will know what to do and what to expect in an emergency
- there will be a clear definition of what a ‘disaster’ looks like for your school or college
- you can test your disaster recovery plan to identify gaps within it

Who needs to be involved

The senior leadership team (SLT) digital lead will be responsible for this standard, but will need input from:

- the operational team (such as finance, IT support and estate management), teaching and other admin staff to understand risks and any actions that can be taken to avoid them
- the designated safeguarding lead, who can advise on safeguarding needs and concerns in the event of a disaster
- the data protection officer to provide advice for mitigating data risks and emergency responses
- governors or trust leadership who will review, support and challenge these plans and provide sign-off, if required
- any outsourced services or suppliers (for example, management information systems, broadband or cloud services) to understand their protocols and include them in plans

How to meet this standard

Digital technology should work with your existing business continuity and disaster recovery plans. To do this you should either include digital technology in your existing plans or have a separate plan for digital technology. Both plans need to be reviewed and updated annually or when a significant change occurs.

Once your plans have been completed, you should create a summary document with top-level details (such as key contacts for when a disaster occurs) to be shared securely with all staff.

The business continuity and disaster recovery plans, including the summary documents, should be:

- printed out to retain hard copies in case of an emergency, such as a cyber incident
- kept online in a secure, shared folder location in the cloud, with remote access granted to those in your disaster recovery team

Disaster recovery Plan

Your disaster recovery plan is a living document to use when a disaster takes place. It should be tested annually (at a minimum) to identify any gaps in knowledge or work needed within your digital technology estate.

It is a set of rules to follow depending on the disaster and should include details such as:

- a definition of what a disaster for digital technology means to your school or college, defined by how long you can function when the disaster takes place
- details of your disaster recovery team and key contacts, including:
    - who they are
    - what they are responsible for
    - their contact details
- how you will test your disaster recovery plan – for example, simulating data loss or hardware failure

Business continuity plan

Your business continuity plan should look at:

- assessing risks of digital technology
- steps that can be taken to reduce risk
- actions that need to be taken if risk occurs and there is a need for recovery

When to meet the standard

Insurance companies may ask all schools and colleges for these documents as part of risk management. So, you should already be meeting this standard or be working towards meeting it.

Related standards

The following links will also help you to meet this standard.

Broadband internet standards

- Schools and colleges should have a backup broadband connection to ensure resilience and maintain continuity of service

Cyber security standards

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

Cloud solution standards

- Make sure that appropriate data backup provision is in place
- Cloud solutions must follow data protection legislation
- Cloud solutions should use ID and access management tools

Filtering and monitoring standards

- Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning
- You should have effective monitoring strategies that meet the safeguarding needs of your school or college

Servers and storage standards

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

Standard 4

Have a digital technology strategy that is reviewed every year

Before you review this standard, please make sure you complete the first 3 standards in this topic called:

- Assign a senior leadership team (SLT) member to be responsible for digital technology
- Keep registers relating to hardware and systems up to date
- Include digital technology within disaster recovery and business continuity plans

Why this standard is important

Creating a digital technology strategy that is aligned with your development plan will help to make sure:

- the digital technology used meets the needs of staff and students
- your budget, buying decisions and any risks are managed
- staff and students receive the training they need to use digital technology safely and effectively
- you can assess the impact of digital technology against your strategy

Not having a strategy in place could lead to:

- disrupted learning if the digital technology does not support curriculum delivery
- potential compromises to safeguarding
- an increased risk of a cyber attack
- budget pressures if digital technology systems fail and need to be replaced
- buying digital technology that is not suitable for the school or college’s educational vision
- a lack of resources (such as the right roles, budget and funding) to support the use and replacement of digital technology

Who needs to be involved

The SLT digital lead is accountable for this standard and will coordinate and manage the digital technology strategy with input from:

- subject leaders, teaching and learning leads, heads of year, and exam officers to understand their teaching and learning needs for both staff and students
- IT support, who will assess the existing hardware and software for whether they are fit for purpose and help identify any potential risks and gaps in resources
- the operational team (for example the school, college or trust business professional, finance team or IT support) to help support and inform budget planning
- designated safeguarding lead and data protection officer to give advice and identify risks and issues related to their roles
- the person responsible for special education needs and disabilities to identify accessibility, diversity and inclusion needs

Your governing body, school board or board of trustees will support and challenge any plans and decisions made on the digital technology strategy.

To create a strategy, you could:

- get input from your own school or college community
- speak to other schools and colleges who have been through a similar process

How to meet this standard

The SLT digital lead will need to understand the school or college's development plan to make sure the digital technology strategy supports this. They will also need to know your current digital technology estate. This should include gathering information on:

- contracts and assets, including physical and data assets
- current and committed digital technology spend
- risks, including disaster recovery plan (contingency planning) and business continuity plan
- what technology students have access to outside of their school or college
- training and development needs for staff and students to be able to meet the vision of the digital technology strategy

Developing a vision

The SLT digital lead should develop a longer-term vision for digital technology to support all educational and organisational needs. The vision:

- should support the school or college's development plan and educational vision
- should be sustainable and minimise the impact on the environment
- could be informed by stakeholders and by visiting other schools and colleges with similar needs to yours

Creating and managing the strategy

Once the vision has been finalised, the SLT digital lead should create a minimum 2-year strategy. This will take into consideration the changes in digital technology and the longer-term plans for what might need to be refreshed or replaced.

The SLT digital lead will also need to:

- revisit and review the strategy annually (at a minimum) and amend it in line with any changes
- share a top-level summary of the strategy to key stakeholders

When to meet this standard

To meet this standard, you will need to have met the previous 3 standards above. Once you have completed those, this standard can then be completed before your next budget cycle.

Related standards

The following standards should also be considered when creating your digital technology strategy:

- cyber security
- filtering and monitoring
- laptop, desktop and tablet
- servers and storage
- cloud
- broadband