

 **Reviewing a Service Level Agreement**

 Updated September 2021

Version 2.0

**This guidance does not constitute or replace legal advice**

**Contents**

[1. What is a Service Level Agreement (SLA)? 2](#_Toc38922647)

[2. Why is an SLA necessary? 2](#_Toc38922648)

[3. What should a service agreement include? 2](#_Toc38922649)

[3.1 Document Control 2](#_Toc38922650)

[3.2 Stakeholders 2](#_Toc38922651)

[3.3 Service Scope 3](#_Toc38922652)

[3.4 Customer Requirements 3](#_Toc38922653)

[3.5 Response Times 4](#_Toc38922654)

[3.6 Service protocols 4](#_Toc38922655)

[3.7 Review and Revision 4](#_Toc38922656)

[3.8 Not meeting agreed service levels 5](#_Toc38922657)

[3.9 Exceptions and Limitations 5](#_Toc38922658)

[Key considerations relating to specific service aspects 5](#_Toc38922659)

[4.1. Scheduled maintenance 5](#_Toc38922660)

[4.2. Telephone support 5](#_Toc38922661)

[4.3. Email support 5](#_Toc38922662)

[4.4. Troubleshooting 5](#_Toc38922663)

[4.5. Remote control, remote assistance, and monitoring. 6](#_Toc38922664)

[4.6. Emergency response 6](#_Toc38922665)

[4.7. On site visits 6](#_Toc38922666)

[4.8. Backup services 6](#_Toc38922667)

[4.9. Filtering services 7](#_Toc38922668)

[4.10. Website hosting / monitoring 7](#_Toc38922669)

[4.11. Antivirus / malware protection 7](#_Toc38922670)

[4.12. Wireless access points 7](#_Toc38922671)

[4.13. Software applications 7](#_Toc38922672)

[4.14 ICT assets 8](#_Toc38922673)

[4.15 Server access 8](#_Toc38922674)

# What is a Service Level Agreement (SLA)?

An SLA is a documented agreement between your IT service provider and your school, as the customer. It identifies both the services required and the expected level of service. The agreement varies depending on the service you are purchasing and will vary from provider to provider. It is important to compare provider service levels when deciding if your service is suitable for your needs or comparative in cost.

Before subscribing for an IT service the SLA should be carefully evaluated to ensure you are getting good value and the services you expect.

# Why is an SLA necessary?

An SLA ensures that you have something to fall back on if a supplier fails to provide services, maintenance, or support. An SLA document sets out all the services to be provided within a supply contract, how reliable they should be, and what measures should be taken in the event of failures or unexpected circumstances.

It should clearly define responsibilities to protect the school in the event that the supplier does not provide the services purchased, or meet the required service levels.

# What should a service agreement include?

**3.1 Document control**

**3.2 Stakeholders**

**3.3 Service scope**

**3.4 Customer requirements**

**3.5 Service management**

**3.6 Service protocols**

**3.7 Review and revision**

**3.8 Consequences of not meeting the SLA**

**3.9 Exceptions and limitations**

## 3.1 Document Control

* Version details
* Document change history, including last reviewed date and next scheduled review
* Document approvals following any amendments
* Review dates

## 3.2 Stakeholders

The SLA should detail school staff who are authorised to request services, order equipment, or make support requests.

The company should state if there is a designated IT Technician, or how available technicians are assigned if support tickets are picked up on a rota system.

## 3.3 Service Scope

The scope details what is covered in the service you are purchasing. This should provide clear delineation of where the IT provider’s responsibility ends and the school’s starts. There are various service aspects to consider:

Telephone support

Email support

Remote assistance

Scheduled maintenance

Troubleshooting

On-site visits

Emergency response

System health checks

Backup services

Filtering services

Website hosting / monitoring

Antivirus / malware protection, and monitoring

**In addition to defining the services to be provided, the contract should also document how the services are to be monitored. This allows the school to assess if services are meeting the agreed levels.**

## 3.4 Customer Requirements

Customer responsibilities may include:

* Payment for all support costs at the agreed intervals (monthly / yearly etc.)
* Availability of school staff when resolving a service related incident or request
* The required reporting time frame for security incidents
* The need for a staff member to manually swap backup drives
* The need for the school to ensure equipment is secured against vandalism / theft (In cases of provider owned / leased equipment)
* Advising the provider when school requirements may necessitate a review, modification, or amendment of the SLA

## 3.5 Response Times

Your SLA should feature information on the availability of any required support. Services provided may have regular operating hours and scheduled times for maintenance. This information needs to be included in the SLA.

Consider what response times you would expect in the following situations:

**Severity Level Description**

a) Outage Server down or cyber-attack in progress

b) Critical High risk of downtime or suspected security incident

c) Urgent End-user impact

d) Important Potential for impact to users if not addressed

e) Routine To be addressed as part of routine support services

f) Monitor Issues addressed / not currently impacting but could

g) Informational Inquiry for information

Define response times for service requests and options regarding remote assistance carefully. Some companies may meet the response times by providing an automated message upon support call receipt.

## 3.6 Service Protocols

Service protocols cover the ways in which service / support requests are communicated to the provider, and how the provider communicates any identified issues to the school.

Protocols set out how you would expect to be informed of a security or network issue from your provider, and the expected timescale. The same is true of how you advise your provider of issues to ensure they have all the required information to respond in a timely manner.

## 3.7 Review and Revision

An SLA should change when the school’s service requirements change. An SLA should not be viewed as a static document and should always include a review date.

Last Review: DD/MM/YYYY

Next Scheduled Review: DD/MM/YYYY

Review is definitely necessary if the technical environment has changed (for example, more equipment is in the scope or there is a move from manual local backup to automated cloud backup). The SLA will avoid misunderstandings, and protect the school should disputes arise.

## 3.8 Not meeting agreed service levels

SLAs may include agreed financial reimbursement for service levels which are not met, credits for further work, or an agreed penalty payment. The SLA should not be used to penalise either party, but it should provide a clear delineation of responsibilities and ensures that the expectations of both parties are met.

## 3.9 Exceptions and Limitations

Read any exceptions and limitations carefully to make sure you understand what is excluded from the service or when the service may be unavailable.

# Key considerations relating to specific service aspects

Schools should follow [Derbyshire Audit Guidance on the Procurement of IT Services](https://schoolsnet.derbyshire.gov.uk/site-elements/documents/administration/finance-and-legal/audit-guidance-on-the-procurement-of-schools-it-systems.pdf) and satisfy themselves their supplier meets minimum professional standards such as ISO 27001 or Cyber Essentials.

The following points are designed to offer assistance in reviewing your service level agreement:

4.1. Scheduled maintenance **and system health checks**

It is important to document what form scheduled maintenance tasks will take, and their frequency. Preventative maintenance must be documented rather than assumed as insurance companies may require evidence of regular maintenance before paying out any claim.

4.2. Telephone support

It is important to verify whether you will have access to a manned service or if an answerphone is in use as this can have support implications. Check how service response times are calculated to ensure a receipt of an automated message is not classed as a response. Service response should be from report time to repair / assessment of further works.

4.3. Email support

Email support may be received by numerous recipients and it is important to clarify how is this monitored and by whom. As with a telephone service, check whether an automated email response is classed as meeting response times.

4.4. Troubleshooting

Be sure to have a process for reporting system faults and put in place a central system to document who reported any issues, and in what timeframe they were addressed. (This helps to check the service against the agreed levels)

4.5. Remote control, remote assistance, and monitoring

Any remote access needs to be clearly defined, detailing how it takes place and documenting the time and reason. Users should be given warning of remote connections and prior to third-party device access. Verify what security is in place for securing connections and ensuring legitimate access. SLAs should record the type of monitoring that takes place and what type of data logs are recording.

4.6. Emergency response

Both parties should be clear as to what constitutes an emergency, and what response time is expected in such situations. If access to the school site is required, ensure there is a way of facilitating this out of school hours.

Ensure there is there a critical incident plan, ideally formulated in liaison with the school’s IT provider. School staff and IT providers should understand their role in the plan and should, as far as possible, test and review it.

4.7. On-site visits

Check whether technicians attending school sites are company employees or whether the company uses or may use sub-contractors. Remember the usual checks and safeguards apply. Verify ID when necessary, and ensure technicians sign in. This also helps to check in / out times for technicians paid by the hour.

4.8. Backup services

The school needs an off-site backup. This could be a backup stored in a separate building or a backup stored in the cloud. If there is a need for staff to change physical backup media, it is vital that this is clearly communicated to the designated staff and there is a contingency in case of staff absence.

Backup success should not be assumed and IT providers should verify backups as successful. Review how often backups are scheduled to run and what data is included in the backup. In a worst case scenario, where a backup may be corrupt or missed, consider how much data would be lost and if this would be acceptable.

All backups should be encrypted and all backup media must be adequately secured. Removable drives can be a target for thieves and servers should be positioned to provide the maximum security possible.

It is important to document which IT personnel have access to the school backup. Remember that anyone with access to your backup has access to the majority of data your school controls. If your IT provider backs up your data they are a data processor and should be registered with the ICO. Due diligence is essential.

4.9. Filtering services

Any SLA should detail what type of filtering service is provided, how it is managed and who is responsible for updating whitelists and blacklists. Have a clearly communicated process for reporting issues with web filtering to be reported and for reviewing logs.

Ensure there is a mechanism for staff to report sites which have been allowed which shouldn’t be. Check there is provision for preventing users from bypassing proxy settings or using virtual private networks. Remember this overlaps with the [Prevent Duty](https://www.derbyshire.police.uk/advice/advice-and-information/t/prevent/prevent/).

4.10. Website hosting / monitoring

If the school is purchasing website hosting be sure that any contracts cover what happens to personal data such as photographs at the end of the contract term.

SLAs should detail what security protects the website from SQL injection (malicious code to access information), malicious scripts, or other types of attack.

Schools should be certain where and how website content is backed up and who is responsible for verifying this.

4.11. Antivirus / malware protection

The service level agreement should include the requirement for the IT provider to report any alerts to the school. The agreement should detail the expected time frame and the anticipated response time. Active monitoring should take place to warn of any threats, and ideally updates should be centralised.

Any incidents or issues should be documented, and mitigations, updates and patching should also be recorded.

4.12. Wireless access points

Wireless access points should have a separate guest login to prevent disclosing the main Wi-Fi code to visitors. The school should be able to change the guest login easily and should have the required information to be able to do this.

4.13. Software applications

Any agreement should specify software provision or updating responsibilities and who is responsible for checking licensing. The school must be clear who can request new software installations and have a record of any software installation.

4.14 ICT assets

Many IT providers use inventory software, run from the server, which detects items which connect to the network. Schools should be aware these lists do not record equipment kept in storage.

Creating this type of asset list may record when and where machines connect. This information can be attributable to individuals and so it is advisable to treat any logs or reports as containing personal data.

4.15 Server access

Schools must document who has access to the school server and the administrative account. The administrator account should only be used to carry out administrative tasks and not used for routine tasks.

At least one member of school staff, preferably two, should have administrative access to the system. This ensures system access can be suspended if disputes or issues arise with the provider. This is also helpful if a critical incident means access is time dependant.