**A Guide to the Cloud**

Released July 2021

Contents

[**1. What is the Cloud? 3**](#_Toc76460333)

[**2. What are the advantages? 3**](#_Toc76460334)

[**3. What are the disadvantages? 4**](#_Toc76460335)

[**4. Cloud computing 4**](#_Toc76460336)

[**5. Public and Private 5**](#_Toc76460337)

[**6. Cloud Security 5**](#_Toc76460338)

[6.1 Due Diligence 5](#_Toc76460339)

[6.2 Policies and Procedures 5](#_Toc76460340)

[6.3 Staff training 5](#_Toc76460341)

[6.4 Data Segregation 6](#_Toc76460342)

[6.5 Strong Authentication Systems 6](#_Toc76460343)

[6.6 Protect Data in Transit 6](#_Toc76460344)

[6.7 Data Masking 6](#_Toc76460345)

[6.8 Device security 6](#_Toc76460346)

[**7. Cloud Backup 7**](#_Toc76460347)

# What is the Cloud?

The cloud is used often in society today, but what is it? The cloud refers to services which are typically provided over the internet. The cloud still uses servers, but they are housed off-site.

Most cloud services can be accessed through your web browser from any internet enabled device. Some providers have dedicated mobile apps to improve access.

Examples of cloud services include:

* Microsoft OneDrive
* Google Drive
* Amazon Cloud Drive
* Apple iCloud
* Netflix
* Dropbox

# What are the advantages?

**Anytime Access**

Cloud services provide many advantages to users. You can access your information on any device with an internet connection. You can edit the same file on multiple devices, making working remotely and from multiple sites simple and efficient, and without the need to transfer the data anywhere.

**Reduced Cost**

You don’t have to procure, run, and maintain the infrastructure. The remote (off-site) servers you use for cloud services are incredibly powerful machines which you do not have to purchase upfront.

Cloud providers can afford to make their services cheaper than you could provide them on-site, by taking advantage of economies of scale and by balancing the needs of different users with different working patterns. You will also only pay for the resources you need.

**Flexibility**

It is easy to expand services and add IT infrastructure, such as data storage, data processing, and memory to upscale your provision without costly installations and disruptive implementation.

**Enhanced Skills**

The company running and securing the cloud services will employ highly skilled and experienced technical staff, meaning that at least in theory, they can deliver more secure and efficient services than you may be able to as a school / educational setting.

# What are the disadvantages?

If you have a site with a poor internet connection or do not have internet enabled technology available, then access to the Cloud is restricted. There is also the possibility that your provider may experience a server outage or technical issue, beyond your control, which affects access to your own information.

There is also the risk that, as your data is being hosted online, it could get into the hands of cyber criminals. Due diligence on your provider is essential to ensure that your minimise the risks.

# Cloud computing

Cloud services can range from the basics of simple storage for one single user, networking and processing functions, standard office and other software functionality, through to artificial intelligence.

There are three distinct cloud computing services:

**Infrastructure-as-a-Service (IaaS)**

This is when settings rent physical or virtual servers, storage, and networking.

*Examples: Cloud backup services from Microsoft Azure or Amazon Web Service (AWS)*

*Also refer to NCSC’s* [*13 IaaS Principles*](https://www.ncsc.gov.uk/collection/cloud-security/iaas)

**Platform-as-a-Service**

This includes infrastructure services and additional applications and tools which help settings to run database management / operating systems and development tools.

*Examples: Netflix and Google App Engine*

**Software-as-a-Service**

The delivery of applications as a service and the most common purchased by schools and educational settings.

*Examples: Cloud-based MIS solutions / applications pupils can access from home*

There is also a fourth option:

**Serverless Computing**.

Serverless computing enables your organisation to access resources ‘as and when’ in response to a demand. With traditional cloud computing, the computer resources are dedicated to you whether you're using them or not.

# Public and Private

Public cloud services are frequently offered in major cities, coffee shops, and places like hotels. They offer convenience. They are cheap or even free but lack oversight, and their use comes with strong security warnings.

Private cloud services are owned by an organisation, or the organisation has exclusive use of them.

# Cloud Security

This should be read in conjunction with the NCSC’s [14 Cloud Security Principles](https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles)

## 6.1 Due Diligence

Any issue with the way the cloud provider manages or secures their services will impact your users. Most cloud providers utilise ‘software defined networking’ (SDN) and this enables networks to be centrally and intelligently controlled, however configuration errors can lead to vulnerabilities. It is essential to carry out due diligence.

Ensure you are satisfied with your provider and make certain that you’ve checked the following:

## 6.2 Policies and Procedures

One of the main challenges with cloud computing is that employees may use a wide range of different personal devices to access school / setting data.

Ensure that you have reviewed the relevant policies, including:

* IT Security Policy
* Bring Your Own Device (BYOD) Policy
* Acceptable Use Policy and *signed* Acceptable Use Agreements

For further reference read the DfE’s [Moving your school to the Cloud](https://www.gov.uk/government/publications/moving-your-school-to-the-cloud/moving-your-school-to-the-cloud) guidance.

## 6.3 Staff training

Staff should all receive basic cyber awareness training and practice good cyber hygiene around password management, device updates, learning to recognise risks, and knowing how to report concerns.

Staff will benefit from guidance around off-site working, which should include the theft of devices, the dangers of using public Wi-Fi, the importance of using a Virtual Private Network (VPN) and shielding screens to prevent ‘shoulder surfing’.

## 6.4 Data Segregation

When utilising cloud technology organisations are sharing a part of a very large resource with other users.

It is essential to ensure that data is reliably segregated from others using the service, and that security is proportionate to the sensitivity and value of the data being accessed, stored, or transferred.

## 6.5 Strong Authentication Systems

Only authorised individuals should be able to access systems and data, and this access should be based on whether the access is needed to do their job.

Just as important here is the provisioning and de-provisioning of access rights and ascertaining the access your provider has to data.

Contracts should cover when it may be necessary for a service provider to access your data and define an approval process / access protocol.

## 6.6 Protect Data in Transit

To preserve the confidentiality of data as it travels to and from your site to provider, protect it at rest (when it is stored), or have strong encryption in place when it is being processed.

Encryption keys ‘unlock’ encrypted data, and decryption requires storage of the encryption keys. To optimise security, the encryption keys should be stored on your own network or on another trusted third-party network, rather than be stored by the provider.

## 6.7 Data Masking

This is to avoid any form of unauthorised disclosure by ‘de-identifying’ the data. For example, any information that helps to identify an individual might be removed or replaced.

This can be done by *obfuscation* to obscure the data, or *anonymisation / tokenisation* to remove sensitive information and replace it with a useless value which can be switched back with a specific ‘token’.

## 6.8 Device security

Cloud computing doesn’t undo the need for device security. An unsecured device with saved passwords will effectively give criminals ‘keys to the kingdom’.

It is strongly recommended that schools / settings follow [Cyber Essentials](https://iasme.co.uk/cyber-essentials-for-schools/) technical controls.

# Cloud Backup

There is a misconception that data in the cloud is ‘backed up’ and this is not necessarily the case.

Cloud **storage** is designed to store data in one centralised location, known as the Cloud.

You can access your data from any device and location with internet connectivity. Users can collaborate on the same files and so it is easy to keep a track of changes and maintain version control.

If you are saving on the school network and manually saving files to cloud storage, without this manual process, then you may lose files which haven’t yet been uploaded.

What happens if a user changes the file in error, or deletes it? Even if Microsoft could search your historic files for that key year 11 exam submission or year 2 project file, it would be like searching for a book in The British Library without a filing system.

Cloud **backups** are indexed, which means, like a library you can find the files you need and restore them in a timely and efficient manner.

File versioning keeps a history of files, which allows the system to understand when changes take place, then mark the newer version and update a central record. This enables users to return to older copies, as and when required.

Cloud backup solutions are designed in a way that means you can easily restore files if you suffer from data loss. Cloud backup is automated and provides reassurance that you can recover from data loss or corruption. This is **not** the same as cloud storage.