

 **Assessing IT Provision**

 Updated September 2021

Version 2.0

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

**Contents**

[IT Provision and Data Protection Implications 3](#_Toc63092358)

[Security Implications 4](#_Toc63092359)

[Types of Services 5](#_Toc63092360)

[1. Managed Services 5](#_Toc63092361)

[2. Contracted, Unmanaged Services 5](#_Toc63092362)

[3. Ad-hoc / On-demand Services 5](#_Toc63092363)

[Contracts and Service Level Agreements 6](#_Toc63092364)

[1. Backup Provision 6](#_Toc63092365)

[2. Recovery and Restoration Services 6](#_Toc63092366)

[3. Email Provision 7](#_Toc63092367)

[4. Internet Connectivity and Filtering 7](#_Toc63092368)

[5. Network setup / Installations 8](#_Toc63092369)

[6. Technical Support and Maintenance 8](#_Toc63092370)

[7. CCTV Systems 8](#_Toc63092371)

[8. Cloud Services 9](#_Toc63092372)

# **IT Provision and Data Protection Implications**

Consider which services your school purchases, who provides them and what personal data could be accessed / affected.

1. Backup Provision
2. Recovery and Restoration Services
3. Email Provision
4. Internet Connectivity and Filtering
5. Network setup / Installations
6. Technical Support and Maintenance
7. CCTV Systems
8. Cloud Services

Educational Technology (referred to as EdTech) is a combination of software and hardware used to facilitate learning. Each system adopted by a school should be independently assessed and is not covered in this guide.

**DPIAs**

A Data Protection Impact Assessment is always needed if the processing of data in a project is likely to result in high risks.

Although you have not yet assessed the actual level of risk, you need to screen for factors that point to the potential for a widespread or serious impact on individuals.

This document details some of the things which may inform your screening and any subsequent DPIA for your IT provision.

When completing a DPIA schools should consider the following:

* Privacy Notices
* Service Level Agreement
* Professional Certifications / Accreditations such as Cyber Essentials / ISO 27001 compliance
* Administration access
* The nature of the work undertaken and likely access to personal data
* Security provisions, including encryption
* Implementing and monitoring technical controls
* The use of sub-contractors by any provider

Derbyshire’s [Audit Guidance for Schools](https://schoolsnet.derbyshire.gov.uk/site-elements/documents/administration/finance-and-legal/audit-guidance-on-the-procurement-of-schools-it-systems.pdf) on the Procurement of IT Systems states:

*“Schools are legally responsible as data controllers for ensuring all reasonable steps have been taken to protect and safeguard personal data including staff and pupil records.*

*Simply asking whether a company is registered with the Information*

*Commissioner’s Office (ICO) for data protection and agreeing to the supplier’s terms and conditions will not be deemed acceptable under the new regulation. Such action could result in fines being imposed on the School in the event of a data breach.”*

As a minimum, schools should have a contract in place with all third party suppliers that hold the School’s staff and pupil personal data, which clearly references both parties’ obligations including data protection.

Data Protection applies to any processing or operations which are carried out on personal data, which include:

|  |  |
| --- | --- |
| **Data Process** | **IT Related Examples** |
| Collection | CCTV / Electronic forms / website contact forms |
| Recording | File servers / EdTech platforms / safeguarding apps |
| Organisation | File servers / MIS  |
| Storage | Server / backup / removable drives |
| Adaptation or alteration | Interactive, live data sets /real-time editing |
| Disclosure by transmission | Email / uploading to the cloud / data sharing with third parties |
| Dissemination or otherwise making available | Restoration / websites / electronic reports / text messaging |
| Combination | Data corruption / data loss |
| Restriction | User access / authentication / encryption  |
| Erasure or destruction | Deletion / cyber-attack / IT incident |

# **Security Implications**

Companies that store and manage sensitive user data and all those software vendors that offer data backup and encryption tools, as well as the necessary equipment to protect networks and operating systems, such as antivirus and firewalls.

*Article 32 – Security of processing*

*Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

*a) the pseudonymisation and encryption of personal data;*

*b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*

*c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*

*d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing*.

# **Types of Services**

It is important to understand if your school has managed services or not.

A provider who is actively managing your network or filtering will have greater access to data than a provider who has limited access for installation / initialisation.

## **Managed Services**

Managed services are supplied under the agreement that the provider is responsible for maintaining and anticipating the need for services.

Provision encompasses a range of processes and functions to improve operations and cut expenses. Services are actively monitored by the provider.

## **Contracted, Unmanaged Services**

Services are provided under a contract in which only the delivery of the service is covered.

In this instance there is no additional on-going support. Security upgrades or additional requirements are not covered and there is no obligation for ongoing maintenance.

## **Ad-hoc / On-demand Services**

Ad-hoc services are provided only when needed and there is no on-going contract. Engagement is for a specific purpose and, usually, for a designated period of time.

#

# **Contracts and Service Level Agreements**

**Contracts** always have a statement of the service(s) to be provided but rarely go into specific service details. A contract is the agreement between you and the provider which should be written and is enforceable by law.

The contract is a legal document outlining the services provided, without specific service details. Some contracts incorporate a Service Level Agreement, most do not.

**Service Level Agreements** are commonly referred to as SLAs.

SLAs should detail not only the services to be provided, but how the client requires them. This includes defining service standards, detailing how services will be monitored and reported on and what should happen if services do not meet the minimum service level.

Having a separate SLA document means you can revise the SLA without having to revise the contract. The contract can just refer to the agreed SLA, reducing admin burdens.

**Understanding School Service Options**

Schools purchase varying levels and types of IT Support. Not all of these will lead to high risk or require a full DPIA.

## **Backup Provision**

Schools must ensure that personal and sensitive data is stored with suitable security, including encryption.

Schools must ensure they can restore access to their data, including when they are subject to a cyber-attack, technical failure, or other disaster affecting their systems.

Backup data must only be accessible to those entitled to view it.

The UK GDPR also requires personal data to be available at all times to the data subject. The school needs to ensure that the data is backed up often enough to closely reflect the live data.

## **Recovery and Restoration Services**

Schools should ensure that data can be restored in a timely manner.

If the school uses a company to backup and/or restore data, they will be handling, managing, and storing your data. This means they are a ‘**data processor**’ and therefore must follow the same data handling and protection rules as you do.

Your supplier should also be registered with the ICO. [You can check the ICO register here](https://ico.org.uk/ESDWebPages/Search).

## **Email Provision**

The data used to create email accounts constitutes personal data.

Email provision can be locally hosted or cloud based. If your provider is using a third-party system, such as Microsoft or Gmail, this is cloud-based and may lead to data transfers out of the UK.

Be sure your email provider is clear about their security, including their ability to enable encryption and the level of encryption provided.

Data subjects should have the right to retrieve their personal data and there should be provision made for this eventuality and to comply with the right to be forgotten (erasure).

## **Internet Connectivity and Filtering**

The Data Protection Act and UK GDPR, requires that service providers must take appropriate measures to safeguard the security of their service.

What ‘appropriate’ means depends on the nature of the risk, the technology available, and the cost.

Service providers must also inform schools of any significant security risks.

*Regulation 5(1A) says these technical measures must at least:*

*(a) ensure that personal data can only be accessed by those legally authorised to view it.*

*(b) protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access, or disclosure*

*(c) ensure the implementation of a security policy with respect to the processing of personal data.*

Filtering must also meet the requirements of The Counter Terrorism and Security Act 2015, which encompasses the Prevent Duty.

The [Prevent Duty Guidance](https://www.gov.uk/government/publications/prevent-duty-guidance) specifies that schools in England and Wales are *"expected to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"*

Further guidance on appropriate filtering can be found on the [UK Safer Internet Centre website](https://www.saferinternet.org.uk/blog/2018-appropriate-filtering-and-monitoring-definitions-published-consultation).

## **Network setup / Installations**

Network installations may lead to data protection compliance issues if administrative logins are shared. If these are provided for a specific project or installation, there should be a record of who has been granted access, who authorised the access, an understanding of how long access is required and a method for removing access when this is no longer required.

Contractors carrying out network cabling installations will not, generally, be provided with admin access to systems. There are unlikely to be any data protection implications for the school, other than the basic considerations which apply to all contractors on the school site.

## **Technical Support and Maintenance**

Technical support services and ongoing maintenance is likely to result on the provision of **administrative access.** Administrative access provides higher access than regular user accounts and can be used to circumvent security processes and controls.

Schools should:

1. Document the appropriate use of administrative access.
2. Specify when it is necessary to use this enhanced level of access.
3. Determine under what circumstances access will be provided and who will authorise it.
4. Have a process to withdraw administrative access, when necessary.

## **CCTV Systems**

The Data Protection Act and UK GDPR applies to any information that can identify someone. CCTV footage includes pictures and videos, which are classed as personal data.

CCTV footage should only be accessible to those who need it to complete a function of their job. This will include staff on site at the school, but could include CCTV monitoring companies or IT support providers who back up the recordings.

Recording security should be documented and include backup schedules and storage.

Schools should also consider necessary access restrictions and protocols, which need to include an access log and a record of authorisation.

## **Cloud Services**

Cloud computing refers to using a computer belonging to someone else (or a company/provider) that you access over the internet. Cloud services may or may not include remote, off-site cloud backup.

The ICO provides information around the data protection [implications of cloud storage.](https://ico.org.uk/your-data-matters/online/cloud-computing/)

The government encourages the use of cloud computing. [The Use Cloud First](Use%20cloud%20first%20-%20GOV.UK%20%28www.gov.uk%29) Policy provides further information.

The school, as the cloud customer, determines the purpose and manner of processing. This means that the school is still the data controller with overall responsibility for complying with data protection legislation.

Schools who are looking to process personal data via cloud services should conduct a privacy impact assessment for the specific platform they intend to use. This should review the guarantees of availability, confidentiality, security, and data integrity that the cloud service vendor provides.

Encryption should be used as a technical measure to secure personal data. Information stored in the cloud may be encrypted in use, in motion (during transfer), or at rest. Be sure your SLA details the level and type of encryption.

Cloud systems may not store data in the UK, giving rise to data protection implications around data transfers. A large cloud provider may have a number of data centres and schools must ensure they are aware of any data transfers, and storage locations, to ensure compliance.

**Annexe 1. Cloud Checklist**

|  |  |
| --- | --- |
| Risks | Make a list of the personal data you hold and how it will be processed in the cloud. |
| Confidentiality | Can your cloud service vendor provide an appropriate third party security assessment? |
| Does this comply with an appropriate industry code of practice or other quality standard? |
| How quickly will the cloud provider react if a security vulnerability is identified in their product? |
| What are the timescales and costs for creating, suspending, and deleting accounts? |
| Is communication encrypted in transit? Encrypted at rest? What level of encryption?  |
| What are the data deletion and retention timescales? Does this include end-of-life destruction? |
| Will the cloud provider delete all of your data securely if you decide to withdraw from the cloud in the future? |
| Will data about users will be shared with third parties or shared across other services the cloud provider may offer? |
|   Integrity | What audit trails are in place so you can monitor who is accessing which data? |
| Does the cloud provider allow you to get a copy of your data, at your request, in a usable format? |
| How quickly could the cloud provider restore your data (without alteration) from a back-up if it suffered a major data loss? |
| Availability | Does the cloud provider have sufficient capacity to cope with demand from other cloud customers and still meet setting needs? |
|  Could the actions of other cloud customers or their users impact on your quality of service? |
| Can you guarantee that you will be able to access the data or services when you need them? |
| How will you cover the hardware and connection costs of cloud users accessing the cloud service when away from school? |
| If there was a major outage at the cloud provider how would this impact on your school? |
| Legal | Do you have a written contract in place with your cloud provider? |
| How will the cloud provider communicate changes to the cloud service which may impact on your agreement? |
| Which countries will your cloud provider process your data in and what safeguards are in place? |
| Under what circumstances will data be transferred to other countries and can this be limited? |

Taken from ICO’s Guidance on the use of cloud computing Version: 1.1