**Suppliers and Security**

Version 1.0

Contents

[**1. Supplier Security 3**](#_Toc76479628)

[**2. Contracts and Service Level Agreements 3**](#_Toc76479629)

[**3. Business Continuity and Disaster Recovery Plans 4**](#_Toc76479630)

[**4. Services and Support 4**](#_Toc76479631)

[**5. Cyber Security Risk Frameworks 4**](#_Toc76479632)

[**6. System Configuration and Security 5**](#_Toc76479633)

[**7. Control User Access 5**](#_Toc76479634)

[**8. Third parties 5**](#_Toc76479635)

[**9. Accountability 6**](#_Toc76479636)

# Supplier Security

#

Schools and settings rely on a whole series of third-party providers to ensure they can function as an organisation and provide the best teaching and learning experience.

These suppliers and service providers can give rise to security risks, which must be carefully assessed and monitored.

Risks will frequently be evaluated and documented in the [Data Protection Impact Assessment (DPIA)](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/), but it is essential that data security forms part of this process.

As with any type of crime, cybercriminals will look for vulnerabilities and will attempt to exploit the weakest link. If you, as a setting, have taken all the correct steps to mitigate security risks but your trusted partner, with access to your data hasn’t, you will be exposed to risks you may have believed had been mitigated.

# Contracts and Service Level Agreements

**Contracts** are legally binding documents. Without this your setting has no redress should problems arise. Contracts define the ‘what and when’ of delivery:

* + the scope of the service being purchased
	+ service provider roles and responsibilities
	+ customer roles and responsibilities
	+ costs/penalties
	+ your rights to continue/terminate the service and end of service provisions
	+ penalties for contract, data, or security breaches

Your **Service Level Agreement** (SLA) should outline the quality of service expected and fleshes out the ‘how’ of service delivery:

* + expected service levels
	+ what will happen if the service levels are not achieved
	+ Data Security and Data Protection - what security standards will be maintained, along with your rights to audit compliance
	+ data storage – security methods for access, transmission, and [data locations](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/)
	+ data sharing – third parties/partners
	+ data retention – including end of service retention and compliance with the ‘right to erasure’, data portability, and storage limitation
	+ disclosure of security vulnerabilities and incidents

# Business Continuity and Disaster Recovery Plans

A **Business Continuity Plan** outlines how a supplier will continue to provide services to you in the event of an incident.

A **Disaster Recovery Plan** outlines how a supplier will restore access, information, or services following an event.

Your ability to function may rely on third-party provision, so it is vital that you are confident in the services you procure.

* Review a copy of both plans (in some instances they may be one document)
* Find out what testing has been carried out, and when
* Ascertain whether plans have ever been enacted and under what circumstances
* Are there estimated timescales for the recovery of service provision following an incident?
* What are the timescales and processes for you to be advised of an incident?

(Be aware that if access to your data is affected, you may need to report this to the ICO)

* Will third parties be used to recover data and what access might they have?

# Services and Support

In addition to business continuity, ensure you review the support times and facilities. Does the supplier understand your needs and offer website chatbots, email contacts, or telephone helplines at suitable times of the day? Review any FAQ sections on the website, are the answers clear, concise, and easy to understand?

What facility exists to report problems / security concerns and how will users be made aware of this?

How does the supplier inform you about security vulnerabilities and support you to mitigate these? Are you expected to keep track of a supplier ‘noticeboard’ or advice page to become aware of issues, or will the supplier be proactive and provide direct advice?

# Cyber Security Risk Frameworks

Has the provider considered the risks and potential vulnerabilities of their services/systems and are these documented and mitigated satisfactorily?

Are they ISO, Cyber Essentials, or NIST Certified?

A security framework helps businesses to protect systems and processes from harm. Do they follow ISACA, Octave, or COSO risk management frameworks?

If your supplier doesn’t follow a framework, have they considered:

* Data protection and the confidentiality or integrity of data when it is stored, used,

or in transit.

* Physical security to prevent unauthorised access and lower risk of cyber-attack.
* Employee training on security threats, data protection, and secure working practices.
* Control user access and privileges and ensure role specific access with a ‘need to know’ only.
* System hardening, updating, anti-virus, and anti-malware to maximise protection.
* Network monitoring to detect incidents and respond effectively.
* Remote access as an organisation (employer/employee) and any access they may have to your system remotely (business/customer).

# System Configuration and Security

* Who will be the system administrator?
* If the supplier issues security advice and guidance on configuration, who will be responsible for ensuring this is followed?
* Is security built-in to the product (privacy and security by design) and, if relevant, is it compliant with the [Children’s Code](https://ico.org.uk/for-organisations/age-appropriate-design/additional-resources/introduction-to-the-childrens-code/)?
* Has there been any vulnerability or penetration testing to make sure the product is protected against threats?
* Data in transit is at greater risk. How is data transmitted?
* What level of encryption is used? Is this used in transit / at rest / both?
* Do you use all the features, and can any be disabled to reduce the number of vulnerabilities?

# Control User Access

* Change any default passwords and remove any unnecessary accounts.
* Enable two factor authentication where possible.
* Set user permissions based on role and need, not ‘in case’. Review these regularly.
* If there is the ability to log and track user activity, will this be turned on or off, and who will have access to the log?
* Do provider employees have access to your data and under what circumstances?

# Third parties

* Have external security assessments been carried out on the product? If so, what were the findings?
* Does the supplier have contractual agreements for sharing data with any third parties and has due diligence been undertaken?
* How is data shared with any third parties and how is confidentiality maintained?

# Accountability

No matter what service you procure, you remain the data owner and are accountable. Make sure you carry out **due diligence**, to make sure that the data you are charged with is secure.

Take the process of carrying out a Data Protection Impact Assessment (DPIA) seriously and don’t simply see it as a ‘tick the box’ exercise. Be sure you have satisfied yourself of the provider’s suitability, their technical and organisational measures, and the details of the service you will receive.

Any issue with the way the third-party manages or secures the services will impact your users.

Official bodies, such as the Information Commissioner’s Office (ICO) can issue fines if they believe appropriate ‘technical and organisational’ measures have not been taken, or that data has been exposed to unnecessary risk.

Cyber insurance may cover your organisation but is unlikely to cover third parties and won’t compensate you in the event that you receive a fine.