

 **IT Provider Checklist**

 Updated September 2021

Version 2.0

Due Diligence requires that we do everything we can to satisfy ourselves that our chosen IT provider is trustworthy, has the resources to meet our needs, will respect privacy and confidentiality, and meet legal their obligations. This checklist is designed to aid you in carrying out due diligence and completing any necessary Data Protection Impact Assessment.

**Consider the following steps:**

1. Define your provision requirements
2. Consider any concerns
3. Gather key information
4. Validate information you are provided with
5. Conduct a risk assessment
6. Evaluate and mitigate any risks
7. Decide on whether to procure the service
8. Ensure contractual obligations are clarified
9. Carry out ongoing monitoring and review service levels
10. Audit on a regular basis

**What type of provision do you need / is being provided?** (This is not an exhaustive list)

|  |  |
| --- | --- |
| **Providers Core Functions** | **Y/N** |
| Service Desk Support |  |
| Network Monitoring |  |
| Device Management |  |
| Cloud Services (managed or unmanaged) |  |
| Filtering |  |
| Procurement |  |
| Installations |  |
| Backup Services |  |
| Restore Functions |  |
| Remote IT Support |  |
| On-site IT Support |  |
| Out of Hours IT Support |  |
| Network Support / Installation |  |
| IT Security |  |
| Cyber Security |  |

**CHECKLIST**

|  |  |  |  |
| --- | --- | --- | --- |
| **1.** | **Supplier Documentation** | **Checked** | **Notes** |
| 1.1 | Is the company registered with [Companies House](https://find-and-update.company-information.service.gov.uk/)? |  |  |
| 1.2 | Have you carried out a contractual review? |  |  |
| 1.3 | Is there a Service Level Agreement (SLA)? |  |  |
| 1.4 | Does the supplier have public liability insurance? |  |  |
| 1.5 | Does the supplier have cyber insurance?**(Note the value of cover)** |  |  |
| 1.6 | Does the supplier have a GDPR compliant privacy notice? |  |  |
| 1.7 | Does the supplier have an appropriate Information Security Policy?  |  |  |
| 1.8 | Do you know who the supplier’s appointed person is for information security? |  |  |
| 1.9 | Does the supplier have an Acceptable Use Policy, and user agreements signed by their staff? |  |  |
|  |  |  |  |
| **2.** | **Compliance Information** | **Y/N** | **Notes** |
| 2.1 | Is the supplier [ICO Registered](https://ico.org.uk/ESDWebPages/Search)? |  |  |
| 2.2 | Does your supplier understand data protection compliance? |  |  |
| 2.3 | Is there evidence of data protection training? |  |  |
| 2.4 | Is there evidence of cyber awareness training? |  |  |
| 2.5 | Do they have Cyber Essentials / ISO 27001 / CiSP Membership? |  |  |
| 2.6 | Do you have documented information about the security measures the supplier adopts? |  |  |
| 2.7 | Do you have an understanding of their professional qualifications / skills? |  |  |
|  |  |  |  |
| **3.** | **User Access** | **Checked** | **Notes** |
| 3.1 | How many individuals will have access to admin accounts? |  |  |
| 3.2 | Do you have an administrator acceptable use agreement signed by all privileged users? |  |  |
| 3.3 | The school should have administrative access in addition to any third-party. Is this the case? |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **4.** | **Remote Access** | **Checked** | **Notes** |
| 4.1 | Will remote access take place? |  |  |
| 4.2 | How will this take place? (access tool/ remote desktop) |  |  |
| 4.3 | Is the remote access solution secure? |  |  |
| 4.4 | Will users be given a notification prior to desktop access? (If relevant) |  |  |
|  |  |  |  |
| **5.** | **Data Sharing / Transfers** | **Checked** | **Notes** |
| 5.1 | Do you have a data sharing agreement? |  |  |
| 5.2 | Does the supplier maintain a ‘Record of Processing Activities’ (ROPA)? |  |  |
| 5.3 | Do you understand what data may be processed by the supplier? |  |  |
| Detail the types of data which will be processed, stored, or transmitted: |
| 5.4 | Will any data be transferred? *e.g. backup* |  |  |
| Detail the **method** of data transfer: |
| Detail the **protections** in place: |
| 5.5 | Where will any data be stored? |  |  |
| *For locations outside of UK you may need to refer to an adequacy agreement, SCCs and additional measures that may be relevant.* |
| 5.6 | Do you know if any of the services being provisioned are outsourced to third-parties? *e.g. backup / email / helpdesk* |  |  |
| **If** the company outsources services, list any sub processors: |
|  |
| **6.** | **Response Times** | **Checked** | **Notes** |
|  | Have you reviewed response times and are you happy they are adequate? |  |  |
| **Service** | **Timescale** |
| Helpline / Service Desk |  |
| Remote Support |  |
| On-site Support |  |
| Crisis / Incident Support |  |
|  |  |
| **7.** | **Availability** | **Y/N** | **Notes** |
| 7.1 | Have you reviewed the supplier’s Business Continuity Plan? |  |  |
| 7.2 | Will geographical location impact service delivery? |  |  |
| 7.3 | Will the company have enough resources to provide support in case of staff absence? |  |  |
| Consider, if using a sole trader, service resilience and whether third-parties may be used. |

|  |  |  |  |
| --- | --- | --- | --- |
| **8.** | **Risk Management** | **Y/N** | **Notes** |
| 8.1 | Are individual information security risks recorded using a risk register? |  |  |
| 8.2 | Has an annual risk assessment been conducted? *(Please record the date)* |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **9.** | **Network Security** | **Checked** | **Notes** |
| 9.1 | Does the supplier have a robust logging system? |  |  |
| 9.2 | Is there active monitoring and control of internet and email access? e.g. spam filters and content filters |  |  |
| 9.3 | Are centrally managed Anti-Virus and Anti-Malware controls deployed? |  |  |
| 9.4 | Is there an established and practiced patching strategy in place? |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **10.** | **Business Continuity** | **Checked** | **Notes** |
| 9.1 | Does the supplier have a business continuity plan? |  |  |
| 9.2 | How often are business continuity plans tested? |  |  |
| 9.3 | Are backup and restore procedures tested on a regular basis? |  |  |
| 9.4 | What is the recovery point objective for the supplier system?(how far back do backups go)  |  |  |
| 9.5 | What is the recovery time objective (how fast can the supplier restore functions) for disaster recovery? |  |  |