This document aims to support you in considering the potential security implications of IT installations.

Ongoing installations are an essential part of providing and improving services to pupils and staff. More recently, schools have been purchasing and installing new systems to meet the requirements and demands of remote learning. These installations have often been implemented at significant speed and with potential security implications.

There are many types of IT Installations which may have security implication including:

* WiFi Installation
* Network Installation
* Projector and Whiteboard Installation

(Interactive boards which connect to the internet directly have security implications)

* Server Installation (on-site or virtualised)
* Computer Suite Installation
* Installing Laptop Trolleys
* Mobile Devices (Tablets such as iPads)
* Software Deployment

**Third Party Provision**

Third-parties may include cloud hosts, cloud-based software solutions, suppliers, technicians and installation engineers. In order to provision new services third party providers may require access to existing systems.

Be sure that responsibilities during a project are clearly defined and that the responsibility of the school and any third-party are well understood and documented.

Consider how you will ensure that third-parties will comply with school policies and procedures. Schools must ensure that providers are aware of business needs and security expectations.

**Consider the Risks**

Change management is vital to make sure that processes are followed, suitable training takes place and that security risks are understood and reduced to a minimal level.

Security risk assessments and a Data Protection Impact Assessments (DPIAs) should consider the risks of the following:

1. Equipment damage
2. Data loss
3. Data corruption
4. Service loss or interruption
5. Harm to personnel during installation
6. Damage to property

**Cyber Essentials and Installations**

New installations may overlap with Cyber Essentials requirements in the following ways:

1. If you will have to temporarily change security settings, allow remote connections or modify firewall settings ensure there is a documented business case for doing so and that the risks are well understood. *(Section 4 - Boundary Protection)*
2. Ensure there is a process for reinstating security settings promptly after the need has passed. *(Section 4 - Boundary Protection)*
3. Ensure firewalls are enabled after installation, where necessary. *(Section 4 – Boundary Protection)*
4. Make sure default passwords are changed. *(Section 5 – Secure Configuration)*
5. Ensure you have updated records, such as the software and hardware inventories, asset registers, administrator log and relevant policies. *(Section 5 - Secure Configuration and Section 7 – User Access)*
6. Understand how any new system will be updated to ensure on-going security compliance and enable automatic updates, where relevant. *(Section 6 – Patch Management)*
7. If a software installation replaced an older package, ensure historic packages are uninstalled. Secure any legacy data or confirm secure data deletion from old systems, if required. *(Section 6 – Patch Management)*
8. User accounts must be provisioned by following an approval process. Any administrative accounts should be provisioned with an audit trail of the request and approval and confirmation of the access given. *(Section 7 – User Access)*
9. Consider whether implementation will require the installer to have additional access / admin rights. If so, ensure any additional rights are revoked at the end of the process. *(Section 7 – User Access)*
10. If new software is being rolled out, has testing taken place, has application sandboxing been used and, ultimately, has it been added to authorised software lists? *(Section 8 – Malware)*

*Failure to apply suitable mitigations and/or procedures could invalidate any cyber insurance.*

**Associated Legislation**

**Data Protection Act 2018** and the **UK GDPR** which covers all aspects of data protection.

The **Network and Information Systems Regulations 2018** which aims to address the threats posed to network and information systems.

**Health and Safety at Work Act (1974)** which puts a responsibility upon employees to keep the workplace safe.

The Electricity at Work Regulations of 1989, Provision and Use of Work Equipment regulations of 1998.

**Waste Electrical and Electronic Equipment (WEEE) Regulations 2013**, which will apply to the decommissioning and disposal of any old equipment.

**Portable appliance testing** (PAT) may also be required one year after implementation.