

 **IT Security Self-Assessment**

 Updated September 2021

Version 2.0

|  |  |
| --- | --- |
| Completed by: |  |
| Role:  |  |
| Date: |  |

|  |  |  |
| --- | --- | --- |
| **Area** | **Further Actions** | **Completed (Date)** |
| Physical Security |  |  |
| Account Management |  |  |
| Virus Protection |  |  |
| Operating Systems |  |  |
| Application Software |  |  |
| Sensitive Information |  |  |
| Data Backup |  |  |
| Awareness & Education |  |  |
| Network Security |  |  |
|  Email Security |  |  |
|  Portable Storage |  |  |
|  Cloud Service |  |  |
|  Incident Management |  |  |
| Disaster Recovery |  |  |

**‘Yes’** answers require no further action.

**‘No’** answers will require investigation and/or remedial action.

|  |  |  |
| --- | --- | --- |
| **AREAS TO CONSIDER** | **YES/NO** | **ACTION REQUIRED** |
| 1. **Physical Security**
 |
| Are devices properly secured when not in use?  |  |  |
| Could devices be accessed by third parties, such as out of school provision or parents? |  |  |
| Are systems labelled with an ultraviolet pen, or other security markings? |  |  |
| Is there a full hardware asset inventory? |  |  |
| Is hardware disposed of with regard to WEEE regulations and data protection requirements with secure data destruction, if necessary?(Waste Electrical and Electronic Equipment) |  |  |
| Account Management |
| Do users have unique and role specific access? |  |  |
| Are default passwords changed promptly? |  |  |
| Is access provided at the lowest level required for users to carry out their role? |  |  |
| Are passwords covered by an appropriate policy, and are minimum 8-character complexity requirements enforced? |  |  |
| Do folders and/or files have access restrictions where appropriate? *(Consider Personnel/Finance/SMT)* |  |  |
| Are user accounts well managed? e.g. provisioning / leaver processes. |  |  |
| Virus Protection |
| Is anti-virus / anti-malware in use? |  |  |
| Are alerts checked and reviewed for actions? |  |  |
| Is the software regularly updated / set to auto update and allowed to run? |  |  |
| Operating Systems |
| Are operating systems, including those on smart phones, workstations, and servers updated with current security ‘patches’ and service packs? |  |  |
| Are operating systems supported and current? |  |  |
| **AREAS TO CONSIDER** | **YES/NO** | **ACTION REQUIRED** |
| 1. **Application Software**
 |
| Are applications / databases configured for security? |  |  |
| Is software purchased from reputable suppliers and are Data Protection Impact Assessments (DPIAs) carried out? |  |  |
| Is there a full software inventory? |  |  |
| Does school policy ensure staff are limited to approved software only? |  |  |
| Do standard user accounts restrict the installation of applications and software? |  |  |
| Sensitive Data |
| Are there suitable technical controls for sensitive data under school control? |  |  |
| Is there a restriction around printing data and is it kept secure and private once in hardcopy form? |  |  |
| Are sensitive files protected adequately with restrictive, role specific access? |  |  |
| Is there a retention policy and a process for retention secure destruction / deletion, as necessary? |  |  |
| Data Backup and Restoration |
| Is data backed up regularly? |  |  |
| Has there been any test restoring data from backup media?  |  |  |
| Is there any offsite / cloud-based back-up?  |  |  |
| Are onsite back-ups in a secure, fireproof area? |  |  |
| Awareness and Education |
| Are signed acceptable use policies in place? |  |  |
| Are staff aware of how cyber / online safety incidents overlap with safeguarding and how to record these? |  |  |
| Has cyber awareness training been delivered to staff? |  |  |
| Are the governors made aware of the issues that require attention? |  |  |
| **AREAS TO CONSIDER** | **YES/NO** | **ACTION REQUIRED** |
| 1. **Network security**
 |
| Are firewalls on and monitored?  |  |  |
| Is there network traffic monitoring? Consider [Police CyberAlarm](https://www.cyberalarm.police.uk/) |  |  |
| Does the server have redundancy e.g. mirrored hard drives, RAID, redundant power supplies? |  |  |
| Is the server sited away from general access? (physical, on-site servers only) |  |  |
| Is the server protected from physical access and how is this ensured? |  |  |
| Are wireless networks secured and have a guest login?  |  |  |
| 1. **Email security**
 |
| Do we have an email policy (possibly as part of an Acceptable Use Policy)? |  |  |
| Is confidential information being encrypted or password protected? Secure file transfer systems are recommended. |  |  |
| Are our staff aware of phishing attacks? |  |  |
| Do staff know where to report suspicious messages? ([Acton Fraud](https://www.actionfraud.police.uk/) / [NCSC reporting](https://www.ncsc.gov.uk/information/report-suspicious-emails)) |  |  |
| Are staff aware that sensitive files should be encrypted, or password protected? |  |  |
| 1. **Portable storage**
 |
| Are staff using portable storage such as USB memory keys etc, aware of the security implications? |  |  |
| Is auto-run disabled for external drives or do you receive a user confirmation message prior to external devices running? |  |  |
| Do policies cover the restriction of mobile storage and any required technical controls? (e.g. encryption) |  |  |
| Are removable media checked periodically for viruses? |  |  |
| Are staff aware that removable media should be manually backed up? |  |  |
| **AREAS TO CONSIDER** | **YES/NO** | **ACTION REQUIRED** |
| 1. **Cloud services**
 |
| Do all cloud services have a contract / service level agreement (SLA)? |  |  |
| Is the physical location of services documented and compliant with Data Protection Act 2018 requirements? |  |  |
| Are the providers encryption methods / VPN / security policy understood and documented? |  |  |
| Is there an understanding of data retention, portability, and data removal processed? |  |  |
| Does the contract cover the termination of services and the secure removal of personal data from the provider’s systems? |  |  |
| 1. **Incident Management**
 |
| Is cyber security on the school’s risk register with an understanding of the related impact? |  |  |
| Are there well communicated and clear reporting mechanisms for incidents / concerns? |  |  |
| Are key stakeholders identified to ensure prompt action / escalation, if required? |  |  |
| Has at least one staff member received incident management training? |  |  |
| Have manual methods of working been considered for emergency situations. |  |  |
| Disaster Recovery |
| Is there a current disaster recovery plan?  |  |  |
| Has the plan been tested?  |  |  |
| Are key staff and contacts identified in relation to disaster recovery? |  |  |
| Is there a communication plan in place for all stakeholders? |  |  |
| Does the plan detail the steps to be taken and by whom? |  |  |
| Have all those with identified roles reviewed the plan and understood their role fully? |  |  |