

**Cyber Risk**

 [Insert School Name]

[Version]

|  |  |
| --- | --- |
| **Last Reviewed** |  |
| **Reviewed By** |  |
| **Next Review Date** |  |

**Contents**

[**1.** **What is Cyber Risk?** 2](#_Toc84255406)

[**2.** **Factors which increase risk** 3](#_Toc84255407)

[**3.** **Factors which reduce risk** 3](#_Toc84255408)

[**4.** **Assessing cyber risk** 5](#_Toc84255409)

[**5.** **Classifying Risks** 6](#_Toc84255410)

[**6.** **Risk Assessment** 6](#_Toc84255411)

[**7.** **Develop your path to enhance your security** 8](#_Toc84255412)

# **What is Cyber Risk?**

Cyber risk commonly refers to any risk of financial loss, disruption, or damage to the reputation resulting from the failure system or security.

This can be the result of malicious attack, deliberate and unauthorised access, or unintentional breaches.

Risks arise from:

* Unauthorised access to your network or devices
* Misuse of information
* Failed processes or procedures
* Data loss
* Disruption of service

# **Factors which increase risk**

* Lack of cyber awareness training for users.
* Staff using school-owned devices with local administrator privileges.
* A lack of user access management.
* Delayed updating and/or old devices which no longer receive updates.
* Staff using personal, unsecured devices and a lack of/outdated Bring Your Own Device Policy.
* Poor physical security for premises and devices.
* A lax policy when it comes to password length, password updating, and sharing passwords.
* Failure to identify critical information and systems and how they are protected.
* Neglecting to regularly review cyber security or relying on third-party provider assurances.
* Poor email practice with a failure to encrypt sensitive messages and insecure access.
* Lack of recording and reporting mechanisms for incidents.
* Employees or customers accessing your system from remote locations with security outside your control.
* Failure to plan effectively for cyber incidents.

# **Factors which reduce risk**

1. Secure culture – a top-down approach to cyber security from Governors/SLT to pupils.
2. Assess the current state of your cyber security - self-assessment or independent audit.
3. Develop IT policies – Acceptable Use, Bring Your Own Device, IT Security, Social Media etc.
4. Incident Response and Disaster Recovery Plans – ensuring critical incident documentation covers cyber incidents.
5. Technology – do you have the technology to protect against and handle a cyber-attack
6. Supply chain risk – Ensure contracts and Service Level Agreements (SLAs) cover disaster recovery and minimum security standards.
7. Governance – is there active monitoring, review of any logs, and a process for recording required actions?
8. Analyse risks – identifying gaps in the current provision and areas for improvement.
9. Benchmark your setting – compare your security against industry standards, such as [Cyber Essentials.](https://iasme.co.uk/cyber-essentials-for-schools/)

You can’t protect anything with only technical controls. Cyber security is the responsibility of *all* staff, and isn’t simply the domain of IT professionals.

Using the example of fire prevention planning and response, you wouldn’t simply rely on the fire service. The following table illustrates the types of controls required:

|  |  |  |  |
| --- | --- | --- | --- |
| **Type of Control** | **Control Definition** | **Fire Example** | **Cyber Example** |
| Administrative | Planning documentation | Fire evacuation plan | Incident Response Plan |
| Technical | Software or hardware mechanisms | Fire alarm | Firewalls, encryption |
| Physical | Actual facilities  | Fire doors and escape windows | Perimeter security, such as locks and fences. |
| Preventative  | Aims to prevent something happening | No smoking signs / policies | Acceptable use and IT policies |
| Detective | Tells you when it is happening | Smoke alarm / heat alarm | [Cyberalarm](https://www.cyberalarm.police.uk/) |
| Deterrent | Discourages or delays the problem | Flame retardant material | Good cyber-hygiene, such as strong passwords. |
| Compensative | Money for financial losses / damage | Insurance | Cyber Insurance(Included with Cyber Essentials) |
| Corrective | Fixes the problem **after** the event | Fire brigade / sprinklers | Backup and restoration processes |
| Recovery | Gets you **operational** again  | Critical incident plan | IT Disaster Recovery Plan |

|  |  |
| --- | --- |
| **Improve**Assess the effectiveness of the plan and adjust the processes accordingly. | **Plan**Defined objectives and strategic direction, supported by policy, and communicated clearly and effectively. |
| **Monitor**Monitor and record progress against the plan considering whether the plan objectives have been met. | **Implement**Execute the plan, assigning and co-ordinating roles and responsibilities. Clear, actionable steps. |

# **Assessing cyber risk**

Assess your ability to handle a cyber-attack, who should be involved, how the setting may be affected, and understand where to get support. Understand what data you hold, where it is, how it is protected and the impact of any potential loss.

Risks are broadly categorised as:

* Strategic
* Tactical
* Operational

Having an independent cyber audit or carrying out a cyber security self-assessment is crucial to being able to understand and mitigate risks.

Assess:

* Security Management and Governance
* Asset Management and Inventories
* Security Architecture
* Data Types and Processing Mechanisms
* Emerging Technologies
* Threat and Vulnerability Management
* Regulation and Policy
* Identity Management
* Incident and Risks Management
* Levels of Awareness and Education

# **Classifying Risks**

Risk management is a methodology to try to take every decision to a mathematical, reasonable, and logical basis.

It is vital that the **impact** and **probability** of all identified risks are considered. Some risks are more likely but may not cause significant disruption.

Using the probability rating and impact rating combined you can classify the risk and give a rating.

For example:

Low risk – temporary access issues to a curriculum app.

Medium risk – loss of non-sensitive planning data, which impacts teaching.

High risk – ransomware attack, encrypting the Management Information System (MIS)

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Assessment** |  |  |  |
|  |  |  |  |  |
|  | 1 = Very Likely5 = Unlikely | 1 = Severe5 = Minor | HighMedLow |  |
| Disaster Scenario | Probability Rating | Impact Rating | Risk Rating  | Mitigations / Alternative Actions |
| Flood |  |  |  | Ensure servers are not located on the floor. Site servers and other computers as far away from water pipes as possible. Moisture detectors can be deployed to provide limited early warning. |
| Fire |  |  |  | Ensure there is an off-site backup. Keep server spaces well maintained, well ventilated, and free from dust.Be aware that cabling / trunking can cause fires in other parts of the building to spread quickly to computer rooms. |
| Vandalism |  |  |  | CCTV used to deter and detect vandalism. Site security should include locks and physically restrict server access. Keys to server rooms should be individual and not generic to a whole department / suite of rooms. |
| Power Failure |  |  |  | UPS remote monitoring and available redundant UPS. |
| Setting Cyber-Attack |  |  |  | Check backup rotations, install security updates, monitor anti-virus and malware solutions. Strong filtering also protects the end users. |
| Supply Chain Attack |  |  |  | Check contracts, Service Level Agreements, and verify supplier backup processes are robust. |
| Loss of Communication / Network Services |  |  |  | WAN redundancy, voice network resilience, and using diversely / alternatively routed trunks for telecoms connections can limit likely communication loss. |
| Loss of Building Access |  |  |  | Arrangement with another school or site to utilise their facilities can support critical systems in the event that school buildings can't be accessed. Also utilise cloud solutions to continue to provide education to pupils and communicate with staff. |

# **Develop your path to enhance your security**

Once the risks have been identified settings can create a path to resilience. This will vary due to factors such as perceived benefits, potential impacts, and budgetary constraints.

|  |  |  |  |
| --- | --- | --- | --- |
| **Quick Wins** | **Priority** | **Planned Change** | **Resilience Target** |
| What can you implement quickly which will improve security?Education is always a great first step. | What can’t wait? Are there high risks which need immediate attention? | Policies, procedures, and rolling updates to devices are most likely to need planning and consultation, and should be scheduled. | When you have implemented the changes required to mitigate the identified risks, you should revisit the assessment again to review security. |

Security is impacted constantly by changes to staffing, technologies, and procedural changes. There is no such thing as a ‘fully resilient’ organisation. It is always a balance of budget, useability, and risk.

Security should always include compliance with legislative requirements and due diligence, especially in providers of systems, services, and support.

Compliance with legislation and regulation is explicit and what we **must** do. Due care and due diligence are what you **should** do, and it is important that the rationale and steps taken as part of due diligence are documented. This may include Data Protection Impact Assessments and verifying suppliers are Cyber Essentials or ISO 27001 certified.

To enhance security all staff should be able to:

1. Recognise cyber threats.
2. Understand how cyber threats may impact teaching and learning and your school as an organisation.
3. Know how to react and report in the event of an attack.

Please refer to the website for more documentation to support cyber resilience: <https://educationdatahub.org.uk/cyber-resilience>