Ashleigh

Primary School

Cyber Security Risk Assessment

Reviewed: September 2025

Review date: September 2026

**British Values**

Through its curriculum, extra-curricular activities, teaching and learning this school will promote British values. By doing so, we will ensure that all learners understand the values that have traditionally underpinned British society. The teaching of these values will promote cohesiveness within our school and community. We will prepare pupils for life in England where the population has an increasingly rich diversity of backgrounds, origins, beliefs and cultures by promoting the values on which our society has been built. By teaching pupils these values we will help all to become good citizens of the United Kingdom of Great Britain and Northern Ireland.

**Race Equality and Racial Harassment**

Implicit in all our policies is a belief in race equality and everything will be done to promote this. We do not tolerate racial harassment. (Refer to School’s Race Equality and Racial Harassment Policies).

**1. Summary**

This risk assessment identifies and evaluates the key cyber security risks facing Ashleigh Primary School. Our school handles a significant amount of sensitive data, including children’s records, staff information, and financial details. The primary threats identified are **phishing attacks leading to data breaches**, **malware/ransomware infections disrupting school operations**, and **accidental data loss by staff**.

The current overall risk level is assessed as **Medium-High**. While some controls like web filtering and antivirus are in place, there are significant gaps, particularly in staff training and formal data handling policies. This report outlines prioritised, practical recommendations to mitigate these risks and strengthen our cyber resilience, ensuring we protect our students, staff, and school reputation.

**2 Scope & Methodology**

This assessment covers all IT systems, data assets, and users within Ashleigh Primary School, including administrative systems (SIMS), curriculum networks, learning platforms (e.g., Purple Mash, Twinkl) and communication tools.

The risk level is calculated using a simple and standard formula:

**Risk = Likelihood x Impact**

Both **Likelihood** (the probability of an incident occurring) and **Impact** (the potential damage to the school) are rated on a 1-5 scale.

| **Score** | **Likelihood** | **Impact** |
| --- | --- | --- |
| **1** | Very Unlikely | Negligible (minor inconvenience) |
| **2** | Unlikely | Minor (short-term disruption, no data loss) |
| **3** | Possible (Could happen) | Moderate (some data loss, operational disruption) |
| **4** | Likely | Major (significant data breach, financial loss, reputation damage) |
| **5** | Very Likely / Certain | Critical (Ofsted/ICO issue, long-term closure, safeguarding failure) |

The final risk score determines the risk level: **Low (1-5)**, **Medium (6-12)**, **High (13-19)**, **Critical (20-25)**

**3. Key Assets at Risk**

We have identified the following critical assets that we must protect:

* **Pupil Data:** Names, dates of birth, addresses, medical information, Special Educational Needs (SEN) details, safeguarding records.
* **Staff Data:** Personal details, payroll information, pension details, performance reviews.
* **School Systems:** Management Information System (SIMS), school network servers, learning platforms, and school website. 💻
* **Financial Data:** School budget, banking details, parent payment system information (e.g., ParentPay, School Spider).
* **School Reputation:** The trust placed in us by parents, governors, and the wider community.

**4. Risk Register**

This table details the specific risks identified, their evaluation, and the proposed actions to mitigate them.

| **Risk ID** | **Risk Description & Scenario** | **Impact** | **Likelihood** | **Risk Score (Level)** | **Existing Controls** | **Recommended Actions & Mitigations** | **Owner** | **Due Date** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CSR-01** | **Data breach via phishing.** A staff member receives a convincing fake email (e.g., appearing to be from the Headteacher or DfE) and clicks a link, entering their password. This compromises student data. | 4 | 4 | **16 (High)** | Email spam filter. | 1. Mandate **annual cyber security awareness training** for all staff using the NCSC's free resources and national College training.  -Run a simulated phishing campaign to test staff awareness.  -Implement **Multi-Factor Authentication (MFA)** on all email and key system accounts. | Headteacher / IT Lead | 31/12/2025 |
| **CSR-02** | **Disruption from Ransomware.** Malware is introduced to the network (e.g., via a malicious email attachment) which encrypts all files on the school server, making SIMS and learning resources inaccessible. | 5 | 2 | **10 (Medium)** | Antivirus software installed on PCs. Daily server backups. | **1. Test backup restoration process** quarterly to ensure it works.  Ensure backups are stored offline or on a separate, isolated network segment so they cannot be encrypted during an attack.  Create a formal Incident Response Plan. | IT Lead / SBM¹ | 31/10/2025 |
| **CSR-03** | **Accidental data loss.** A staff member saves sensitive student data (e.g., an SEN register) onto an unencrypted personal USB drive to work from home and subsequently loses the device. | 4 | 3 | **12 (Medium)** | Acceptable Use Policy (AUP) advises against this. | 1. **Ban the use of personal/unencrypted USB drives** for sensitive school data. Provide staff with school-approved, encrypted USB drives if required. Promote the use of the school's secure remote access solution or cloud storage (e.g., Google Drive/OneDrive) instead. | Headteacher | Immediate |
| **CSR-04** | **Weak password compromise.** An external learning platform used by the school is breached. A staff member reused their simple school password, giving an attacker access to their school account. | 3 | 4 | **12 (Medium)** | AUP mentions password security. | Implement a **strong password policy** (minimum 8 characters, no common words).  Ensure MFA is enabled wherever possible (see CSR-01). | IT Lead | 31/01/2026 |
| **CSR-05** | **Unauthorised access by pupils.** A pupil gains access to a teacher's unlocked computer during lunchtime and accesses inappropriate content or other students' files. 🎓 | 3 | 3 | **9 (Medium)** | Classroom management. Web content filtering. | 1. Enforce a school-wide policy for **all staff to lock their computers** (Windows key + L) whenever they leave them unattended.  Re-communicate this policy in staff briefings. | All Staff | Immediate |

¹*SBM = School Business Manager*

**5. Summary of Recommendations**

To effectively reduce our cyber security risk, the following actions should be prioritised:

1. **Continue Mandatory Staff Training:** Roll out the NCSC's cyber security awareness training (National College) for all staff (and Governors) before the end of the year. This is the single most effective control to reduce our vulnerability to phishing.
2. **Deploy Multi-Factor Authentication (MFA):** Immediately begin the process of enabling MFA on all staff email accounts and critical systems like SIMS/CPOMS.
3. **Strengthen Data Handling Policies:** Formally ban the use of unencrypted removable media for any sensitive data and enforce the use of secure, school-approved data storage solutions. Unencrypted removable media could still be used for delivery of lessons, but no children’s data including reports, must be stored on unencrypted media.
4. **Verify Backup & Recovery:** transfer over to an online server, including backups to ensure we can recover from a catastrophic failure like ransomware.

By implementing these measures, Ashleigh Primary School can significantly improve its security posture and better fulfil its duty to protect the data and digital wellbeing of our entire school community.