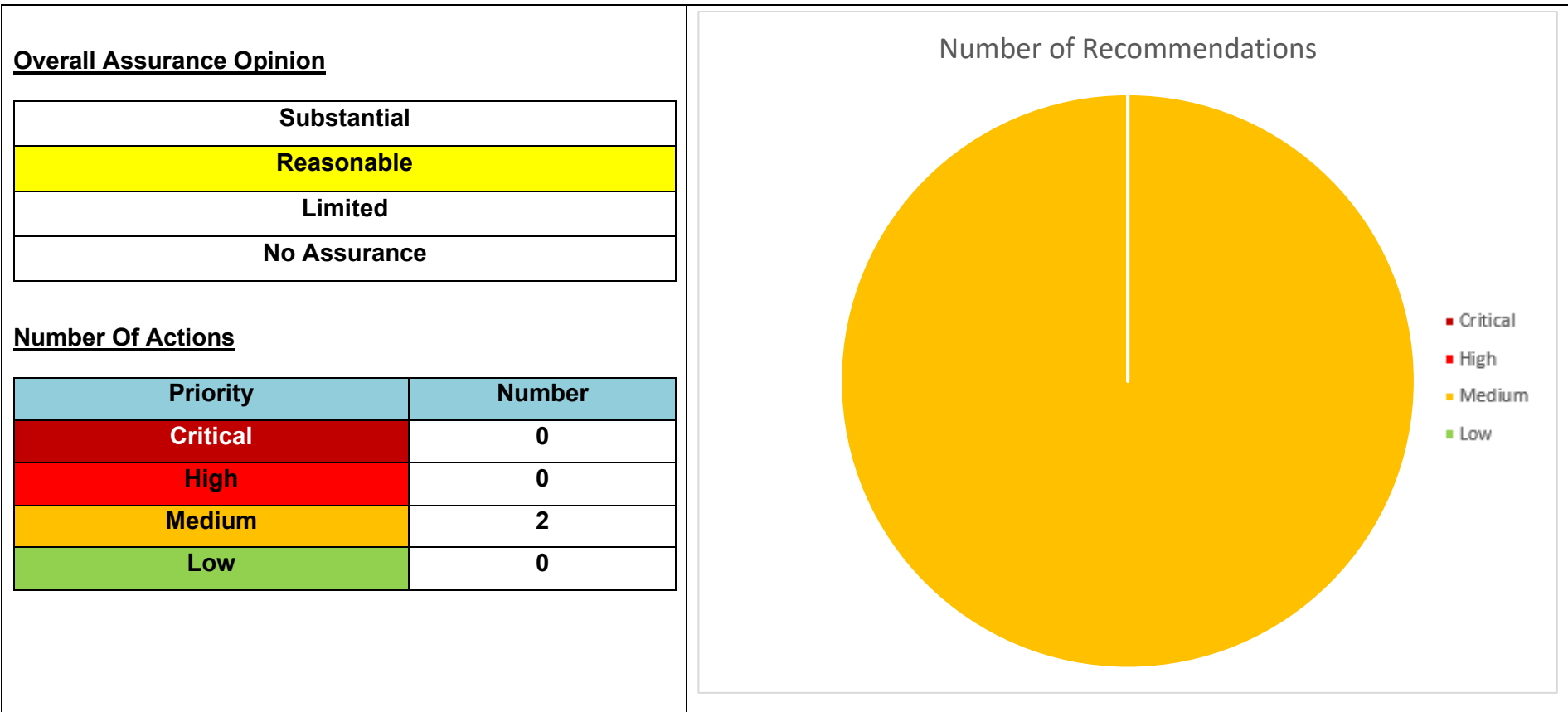


**Internal Audit Report  
Village Infants' School  
24 October 2025**

<b>To</b>	Yolanda Cattle	Headteacher
	Susan Joy	School Business Manager
	Harriet Spoor	Chair of the Governing Body
	Elaine Allegretti	Director of People and Resilience
	Jane Hargreaves	Commissioning Director
<b>From:</b>	Bash Fowora	Internal Audit Manager
	Natasha Prior	Principal Auditor
	Jaimmie Boateng	Internal Audit Apprentice

We would like to thank management and staff for their time and co-operation during the course of the internal audit.

## 1. Executive Summary



### **Audit objective and scope**

The objective of this audit was to ensure that Village Infants’ School, “the School”, has adequate and effective controls with regards to the financial management and governance of the school. Specifically, the review considered the following areas:

- Procurement and Expenditure: Legitimate transactions are made in accordance with the schools purchasing guidelines and achievement of value for money demonstrated.
- Banking and Income: Bank accounts are well managed while income is accurately recorded and accounted for.

- Budgetary Control: There is an adequate framework to set, monitor and report on the school's delegated budget.
- System Control & Data Protection: Information is held securely and access to information are restricted to authorised personnel at all times.
- School Funds: The school fund is well managed and there are independent assurances over the activities related to the funds.

An extract from the Terms of Reference detailing the scope of this review is available at Appendix C below.

### **Summary of approach and findings**

We previously audited the Village Infants School in May 2022, where it also achieved a 'Reasonable' assurance rating, therefore displaying a sustained control environment. Our current assurance level definitions are available in **Appendix A** of this report.

Village Infants' School is for children aged 3 to 7 years old.

The closing balance for the 2024/25 financial year was £51,189. The 2025/26 budget approved by the governing body and submitted to the Local Authority Finance Team in May 2025, projects a revenue income of £2,421,083 and an expenditure of £2,460,616.

The school's three-year financial forecast anticipates a cumulative surplus of £136,847. It was confirmed by LBBB Finance Department that the Ratified Budget and Three-Year Budget Plan was submitted by the school's finance team. There, however, has not been formal communication issued back to the school regarding their budgets.

A review of the school's governing body meeting minutes from May 2025 confirmed that monthly budget monitoring is in place, with measures taken to address any budget variances such as overspending or underspending.

The school adheres to the financial management and standards procedures stipulated in the Council's Financial Policy. This guidance outlines procurement processes schools should follow, and the Financial Scheme of Delegation details levels of approval required for expenditure transactions.

The Arbor Finance Management System is used by the school for invoice processing and payments to suppliers.

Following a review of sample of twenty invoice transactions, the audit identified one instance where a payment was made after its due date, with a valid reason provided for the delay.

The school maintains three bank accounts with Lloyds Bank: a main school account, a ParentPay account, and a school fund account, none of which have an overdraft facility as it is not needed. Additionally, the School Business Manager and Deputy Headteacher each hold a Lloyds Bank charge card, with cash withdrawal functionality disabled.

Audit established that bank statements for the bank accounts are received and reconciled monthly, with the Headteacher reviewing and signing off each reconciliation.

There is a Letting Policy in place, but there are currently no lettings operated by the school.

The school is registered with Information Commissioner's Office for data protection until November 2025 and the role of Data Protection Officer is outsourced to third party, Data Protection Enterprise Ltd.

There are several data and information policies in place that makes up the school's information security policy and available on the school's website.

Audit established that access to the school computer network is username and password controlled, however there are no strength requirements for passwords. Audit found that the school computer system screen lock and sleep are configured to activate after thirty minutes of inactivity.

Audit established that the School Fund is operated separately from the main school account, and accounts were independently audited annually as outlined in the recommendations stated in the Council's Financial Regulations & Standing Orders for Schools.

A sample of sixteen School Fund transactions were selected for review and it was established that all payments were of benefit for the school.

We identified two medium risk findings:

- Computer Screen Lock and Sleep Settings: The current system configuration activates screen lock and sleep mode after thirty minutes of inactivity, which may be considered excessive and could pose a security risk.
- Password Strength Requirements: There are currently no enforced criteria for password complexity, such as minimum length or the inclusion of letters, numbers, or special characters.

## 2. Findings and Action Plan

REF	FINDING	RISK	RISK CATEGORY	PROPOSED MANAGEMENT ACTION	RESPONSIBLE OFFICER TARGET DATE
1.1	<p><b><u>Computer Lock Screen &amp; Sleep</u></b></p> <p>The audit confirmed that access to the school network is controlled through username and password authentication.</p> <p>However, the computer screen lock is configured to activate after thirty minutes of inactivity.</p>	<p><b>Risk:</b> A thirty-minute inactivity period before screen lock activates increases the window of opportunity for unauthorised access, especially in shared or open-access areas.</p> <p><b>Impact:</b></p> <p>Accidental or malicious access to sensitive data by pupils, visitors, or unauthorised staff.</p> <p>Data loss or manipulation, especially if systems are left unattended.</p> <p>Non-compliance with best practices for IT security in educational settings.</p>	Medium	<ul style="list-style-type: none"> <li>Configure all school computers to activate screen lock after 5 minutes of inactivity. This significantly reduces the window for unauthorised access, especially in shared or open-access areas such as classrooms, libraries, or staff rooms.</li> <li>Ensure that all devices are set to automatically lock without requiring user action. Prevents situations where users forget to manually lock their screens when stepping away.</li> <li>Use Group Policy Objects (GPOs) or equivalent tools to enforce screen lock settings across all devices. Ensures consistency and prevents users from altering security settings.</li> </ul> <p><b>Management Action</b></p> <p>School's IT Technician has instructed our ICT Provider to configure screen lock after 5 minutes for the Headteacher, Deputy Headteacher, School Business Manager, SENDCo and all computers in the school office. Computers in the classrooms for teacher will remain at 30 minutes. This will be in place for the start of the Autumn Term 2025/26</p>	IT Technician September 2025

REF	FINDING	RISK	RISK CATEGORY	PROPOSED MANAGEMENT ACTION	RESPONSIBLE OFFICER TARGET DATE
1.2	<p><b><u>Password Strength Requirements</u></b></p> <p>Access to the School's network is username and password controlled.</p> <p>Audit established that that there are no defined password strength requirements for accessing the school network.</p> <p>Users are not required to set passwords with a minimum length or include a combination of uppercase and lowercase letters, numbers, or special characters.</p> <p>As a result, passwords may lack sufficient complexity, making them more vulnerable to being guessed or compromised.</p>	<p><b>Risk:</b> Without enforced password strength requirements (e.g. minimum length, use of numbers/symbols), user accounts are more vulnerable to being compromised through simple or brute-force attacks.</p> <p><b>Impact:</b></p> <ul style="list-style-type: none"> <li>• Data breaches involving sensitive pupil, staff, or parent information.</li> <li>• Unauthorised access to school systems or communications.</li> <li>• Violation of data protection regulations (e.g. UK GDPR), potentially leading to fines or reputational damage.</li> </ul>	Medium	<p>Management should develop and enforce a formal Password Policy that outlines minimum requirements for password strength.</p> <p>Suggested Standards:</p> <ul style="list-style-type: none"> <li>• Minimum of 12 characters</li> <li>• Inclusion of uppercase and lowercase letters</li> <li>• At least one number and one special character</li> <li>• Avoiding using personal information such as birthdates and words that are easy to guess; and</li> <li>• Avoiding simple variations of a current password when creating a new password.</li> </ul> <p><b>Management Action</b></p> <p>SLT to develop a formal Password Policy to be approved at the Autumn Term GB Meeting.</p> <p>ICT provider to implement recommended standards for minimum of 12 characters, upper and lower case and one special character for the start of the Autumn Term.</p>	SBM 23/10/25

## Appendix A: Definition of risk categories and assurance levels in the Executive Summary

Risk rating	
<p><b>Critical</b></p> <p>●●</p>	<p>Immediate and significant action required. A finding that could cause:</p> <ul style="list-style-type: none"> <li>• Life threatening or multiple serious injuries or prolonged workplace stress. Severe impact on morale &amp; service performance (e.g. mass strike actions); or</li> <li>• Critical impact on the reputation or brand of the organisation which could threaten its future viability. Intense political and media scrutiny (i.e. front-page headlines, TV). Possible criminal or high-profile civil action against the Council, members or officers; or</li> <li>• Cessation of core activities, strategies not consistent with government's agenda, trends show service is degraded. Failure of major projects, elected Members &amp; Senior Directors are required to intervene; or</li> <li>• Major financial loss, significant, material increase on project budget/cost. Statutory intervention triggered. Impact the whole Council. Critical breach in laws and regulations that could result in material fines or consequences.</li> </ul>
<p><b>High</b></p> <p>●</p>	<p>Action required promptly and to commence as soon as practicable where significant changes are necessary. A finding that could cause:</p> <ul style="list-style-type: none"> <li>• Serious injuries or stressful experience requiring medical many workdays lost. Major impact on morale &amp; performance of staff; or</li> <li>• Significant impact on the reputation or brand of the organisation. Scrutiny required by external agencies, inspectorates, regulators etc. Unfavourable external media coverage. Noticeable impact on public opinion; or</li> <li>• Significant disruption of core activities. Key targets missed; some services compromised. Management action required to overcome medium-term difficulties; or</li> <li>• High financial loss, significant increase on project budget/cost. Service budgets exceeded. Significant breach in laws and regulations resulting in significant fines and consequences.</li> </ul>
<p><b>Medium</b></p> <p>●</p>	<p>A finding that could cause:</p> <ul style="list-style-type: none"> <li>• Injuries or stress level requiring some medical treatment, potentially some workdays lost. Some impact on morale &amp; performance of staff; or</li> <li>• Moderate impact on the reputation or brand of the organisation. Scrutiny required by internal committees or internal audit to prevent escalation. Probable limited unfavourable media coverage; or</li> <li>• Significant short-term disruption of non-core activities. Standing orders occasionally not complied with, or services do not fully meet needs. Service action will be required; or</li> <li>• Medium financial loss, small increase on project budget/cost. Handled within the team. Moderate breach in laws and regulations resulting in fines and consequences.</li> </ul>
<p><b>Low</b></p> <p>●</p>	<p>A finding that could cause:</p> <ul style="list-style-type: none"> <li>• Minor injuries or stress with no workdays lost or minimal medical treatment, no impact on staff morale; or</li> <li>• Minor impact on the reputation of the organisation; or</li> <li>• Minor errors in systems/operations or processes requiring action or minor delay without impact on overall schedule; or</li> <li>• Handled within normal day to day routines; or</li> <li>• Minimal financial loss, minimal effect on project budget/cost.</li> </ul>
Level of assurance	
<p><b>Substantial</b></p> <p>●</p>	<p>There is a sound control environment with risks to key service objectives being reasonably managed. Any deficiencies identified are not cause for major concern. Recommendations will normally only be Advice and Best Practice.</p>
<p><b>Reasonable</b></p> <p>●</p>	<p>An adequate control framework is in place but there are weaknesses which may put some service objectives at risk. There are Medium priority recommendations indicating weaknesses, but these do not undermine the system's overall integrity. Any Critical recommendation will prevent this assessment, and any High recommendations would need to be mitigated by significant strengths elsewhere.</p>
<p><b>Limited</b></p> <p>●</p>	<p>There are a number of significant control weaknesses which could put the achievement of key service objectives at risk and result in error, fraud, loss or reputational damage. There are High recommendations indicating significant failings. Any Critical recommendations would need to be mitigated by significant strengths elsewhere.</p>
<p><b>No</b></p> <p>●</p>	<p>There are fundamental weaknesses in the control environment which jeopardise the achievement of key service objectives and could lead to significant risk of error, fraud, loss or reputational damage being suffered.</p>

## **Appendix B: Internal Audit Roles and Responsibilities**

Internal Audit is responsible for this report; however, the actions / implementation of the matters raised in this report are only those that came to our attention during the course of our internal audit work and are not necessarily a comprehensive statement of all weaknesses that exist nor all improvements that might be made:

- Management are responsible for maintaining effective internal controls including the implementation of audit recommendations and the management of risks attached to this system / service. Internal audit work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.
- The responsibility for effective and timely implementation of the recommendations made rests with management and these should be fully assessed for their full impact before they are implemented.

## Appendix C: Terms of Reference Extract – Scope of the Review

The audit will consider the potential risks set out in the table below:

Objectives	Risks
<p><b>Procurement and Expenditure</b></p> <p>Procurements are made in line with the school's approved procurement framework and legislation.</p> <p>The best value for money are obtained from any contracts the school enter into.</p> <p>Expenditure on goods and services are made in line with the school's financial regulations and guidelines.</p>	<p>Poor procurement decisions and a failure to comply with procurement framework and legislation could result in:</p> <ul style="list-style-type: none"> <li>• legal challenges from suppliers;</li> <li>• contracts being cancelled and;</li> <li>• financial penalties.</li> </ul> <p>This can be costly, time-consuming and impact on the school's and council's reputation.</p> <p>Contract not in place with appointed Suppliers.</p> <p>Inappropriate goods or services are purchased.</p> <p>Goods and services paid for are not received.</p>
<p><b>Banking and Income</b></p> <p>School bank accounts are administered effectively and reconciled to the school accounting system on a regular basis.</p> <p>All incomes due and received are accurately recorded by the school and paid into the school's bank accounts.</p>	<p>Inappropriate or inaccurate transactions via the school's bank account are not identified.</p> <p>Income is not maximised due to failure to charge in line with policy.</p> <ul style="list-style-type: none"> <li>• Income is not accurately recorded and timely banked.</li> </ul>
<p><b>Budgetary Control</b></p> <p>The school's budget are reviewed, planned, forecasted, implemented and evaluated in accordance with the existing financial regulation and reported on to the Governing Body and the Council.</p>	<p>Budget planning is not robust, and the budget set is unrealistic or is not consistent with the strategic aims of the school.</p> <ul style="list-style-type: none"> <li>• Budget monitoring does not provide adequate information about financial performance or there is insufficient scrutiny to ensure that performance is effectively managed.</li> </ul>

**INTERNAL AUDIT – Village Infants' School Review Report**

<p><b>System Control &amp; Data Protection</b></p> <p>There are set of procedures and technological measures at the school to ensure secure and efficient operation of information.</p>	<p>Inappropriate or unauthorised access may be gained to the school's data.</p> <p>Fraudulent transactions may be created through a lack of appropriate segregation of duties.</p> <ul style="list-style-type: none"><li>• Where adequate logs are not maintained, then inappropriate use/modification of the system or unauthorised access attempts may be untraceable.</li></ul>
<p><b>School Funds</b></p> <p>Monies obtained from contributions or donations from sources other than the Local Authority (LA) are kept completely separate from the Official Fund, have independent records and their own bank accounts.</p> <p>An annual statement is produced and independently reviewed by School's Governing Body appointed person.</p>	<p>Unofficial funds received unaccounted for by the school.</p> <p>Inappropriate and fraudulent used of the unofficial funds.</p>