Juniper

Internal Scrutiny Annual Report

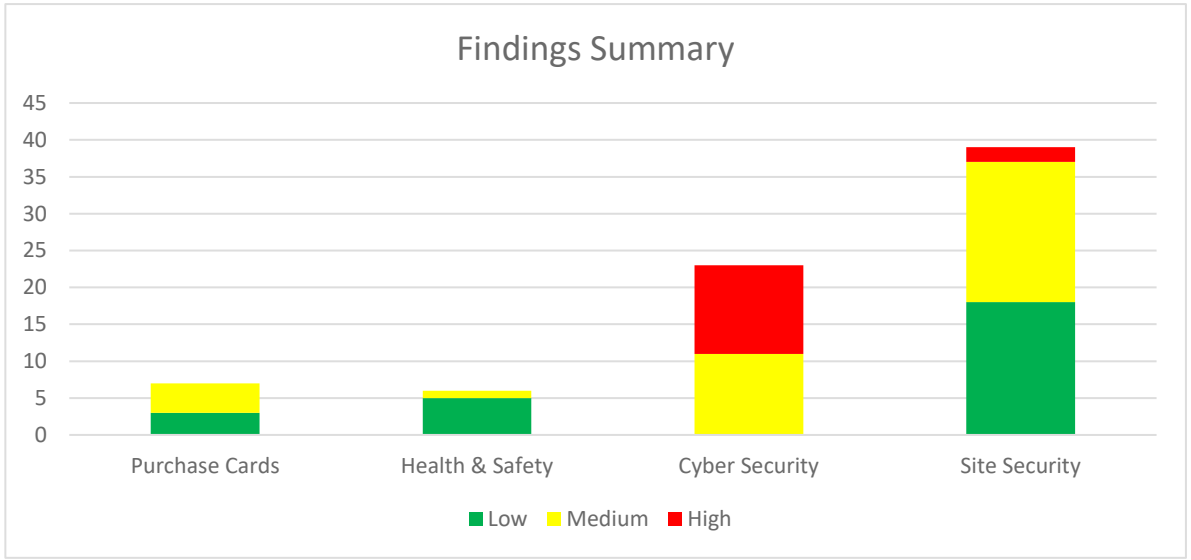
2023-24

Hatfield Community Free School

0345 200 8600 | enquiries@juniperedu cation.org | juniperedu cation.org

Executive Summary

Reviews undertaken:	Review provided by:	Overall Opinion: Good
Financial Control (Purchase Cards): May 2024	Juniper Education	
Non-Financial Control (Health & Safety): Apr 2024	Juniper Education	
Non-Financial Control (Cyber Security): Sep 2024	Secure Schools	
Non-Financial Control (Site Security): Oct 2023	Pharos Response	



Total number of recommendations:	
High Priority	14
Medium Priority	35
Low Priority	26

This report provides assurance that adequate controls are being operated within the trust, based on the understanding that the information provided during the review is accurate and complete. It should be noted however that recommendations to improve controls, if implemented, cannot guarantee that fraud or misappropriation could not occur.

Recommendations raised in the report issued should be considered by the board of trustees / Audit and Risk Committee to assist them in providing assurance over the suitability of, and compliance with, the systems and operational controls in place.

No fraud was identified or reported to us for the 2023-24 period. It remains the responsibility: of management to manage the control environment to help identify potential fraud and prevent the likelihood of fraud occurring.

Juniper

Overall Opinion Criteria

Good	There is a sound system of internal control designed to manage risks.
Satisfactory	There is generally a sound system of internal control processes.
Requires Improvement	There are significant weaknesses in key areas in the systems of control, and a high number of high-risk recommendations have been identified in each review completed.
Poor	Many risks identified are of a high-risk nature, and there are significant process failings.

Juniper

Introduction

The Academy trust handbook specifies

> *3.1 All academy trusts must have a programme of internal scrutiny to provide independent assurance to the board that its financial and non-financial controls and risk management procedures are operating effectively.*

Providing that the trust has selected a scope of work for financial and non-financial controls and has considered its risk register, this Internal Scrutiny Report demonstrates how the trust meets the Academy trust handbook 2023 internal scrutiny requirements.

Please note that this report is an exception report and therefore only contains the details of any issues arising from the review of the scope of work detailed below.

Juniper

Scope & Priority Key

The relevant board, informed by its risk register approved the below scope of work:

Financial Control:

Credit Card Bespoke
Review to establish the effectiveness of controls and processes for all areas of procurement.
Credit Card Processes
Authorisation levels
Policy
Expenditure sample testing
Value for Money
Unresolved issues

High Priority	Issues where there is a risk of significant financial impact on the trust that must be addressed immediately by the academy trust
Medium Priority	Issues where there is a risk of moderate financial impact on the trust, such as a control failure or the absence of a control in an area of moderate risk. These should be addressed soon.
Low Priority	Issues that relate to minor control deficiencies or enhancements in control efficiency. These should be addressed within an agreed timescale.

Juniper

Non-Financial Control (Health & Safety):

Health & Safety
A health & safety audit will consist of two parts; a remote review of the following areas, followed by a physical site inspection:
Policies & procedures
Risk Assessments
Safe Systems of work and communication
Staff training
Record keeping
Site Inspection

Juniper

Risk Level	Description	Action Priority
Immediate	These risks are unacceptable. Substantial improvements in risk controls are necessary, so that the risk is reduced to an acceptable level.	The work activity should be halted until risk controls are implemented that reduce the risk so that it is no longer very high. If it is not possible to reduce risk the work should remain prohibited. It is essential that these issues are resolved immediately.
High	Substantial efforts should be made to reduce the risk. Considerable resources might have to be allocated to additional controls. Arrangements should be made to ensure that the controls are maintained, particularly if the risk levels are associated with extremely harmful consequences and very harmful consequences.	Risk reduction measures should be implemented urgently within a defined time period, and it might be necessary to consider suspending or restricting the activity, or applying interim risk controls, until this has been completed. It is advised that these issues are resolved within 1 month
Medium	Considerable efforts should be made to reduce the risk. Where the risk has been reduced but sufficient documentation is not in place, this must be implemented and retained. Arrangements should be made to ensure that the controls are maintained, particularly if the risk levels are associated with harmful consequences.	The risk reduction measures should be implemented within a defined time period. It is advised that these issues are resolved within 2 Months.
Low	Consideration should be given as to whether the risks can be lowered, but the costs of additional risk reduction measures should be considered (in terms of time, money, and effort). Arrangements should be made to ensure that the controls are maintained.	It is advised that these issues are resolved within 3 months

Juniper

Non-Financial Control (Cyber Security):

Cyber Security Audit
A review to establish the level in which your school or trust is fulfilling its duties and responsibilities concerning cyber security.
Understanding your school or trust
Leadership, risk management & governance
Information assets & risk management
Managing cloud services
Data protection- data security (optional)
People
Cyber Security policy
Change management
Security testing, audit & assurance
Incident management, continuity & recovery

	Essential measures that address immediate and high-level cybersecurity risks.
	Actions that focus on strengthening cybersecurity over a longer term.

Juniper

Non-Financial Control (Site Security):

Site Security
This includes a review of your policies and procedures and a detailed site survey to establish priorities, threats, challenges, and weaknesses. Your detailed report will provide practical advice, realistic recommendations and template documents covering:
alarms and monitoring systems
access control
visitor management
lockdown
emergency communications
VIPs
premises layout
crisis response plans

Juniper

Summary of Findings

Extract from the Financial Procedures Manual - 9.3.1 Corporate Cards

"Unless specifically authorised in writing by the Principal, no member of staff other than staff with financial responsibilities may place orders electronically through the internet. Internet orders should be authorised and input to the accounting system in the normal way. For orders, (such as internet orders and where payment is made in person) where invoiced payment is not possible, the HCFS credit card should be used as payment at the time of ordering, on express authorisation of the Principal." (1)

"The following process is in place to reconcile the monthly credit card statements:

- Corporate card statements are received monthly by the SBM and will be passed to the relevant card holders.
- It will be the credit holder's responsibility to ensure they have all their paperwork at the end of the month so that they can tick off each itemised item on the credit card statement (the PA will complete the Principal's on their behalf).
- Each credit card item purchased, should have a 'credit card slip' which has been signed by both the relevant budget holder and the owner of the credit card. (2)
- Each credit card holder will need to sign their monthly 'Expense Confirmation Form' from Lloyds once reconciliation is complete to verify that all the expenditure is approved and has been accounted for. (3)
- All credit card invoices will be entered onto sage by the Office Manager (with the support of the PA) and then passed to the SBM for month end reconciliation and signing off. (4)

The balance on the corporate card is taken by the bank by direct debit on a monthly basis.

The school charge cards must not be used for personal purchases and must be fully supported by appropriate receipts."

Juniper

RAG	Finding	Recommendation	
Financial Control - Purchase Cards			
Medium Priority	The Financial Procedures Manual (9.3.1) states "Names of card holders and their authority limits: • Principal: £5,000 (single transaction limit of £3,000) • AVPs: £500 • PA: £2,000 • Office Manager: £5,000 • Site Manager: £1,000 The Corporate cards overall limit is £15.5k (not currently fully utilised) and expenditure against this limit should be monitored by the SBM and checked to see if any misuse has occurred." The statement for the Principal's card showed a credit limit of £7,000 and the total credit limit of the 5 cards reviewed totalled £15.5k. It was advised that the academy holds a card for a staff member currently on leave and a further card has been ordered for the School's Vice Principal. The addition of credit available on these cards will breach the overall limit.	The limits set out in the Financial Procedures Manual should be adhered to and the credit limits currently in breach rectified and monitored as soon as possible. These limits should not be exceeded even if a card is not currently in use.	
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Medium Priority	The Financial Procedures Manual states “the HCFS credit card should be used as payment at the time of ordering, on express authorisation of the Principal” (see item 1 from extract above). It could not always be evidenced that the Principal had approved items of expenditure.	Evidence of the Principals authorisation should be retained for every transaction.	
Management Response:		*Responsibility / Due Date:*	
Low Priority	The Financial Procedures Manual states “Each credit card item purchased, should have a ‘credit card slip’ which has been signed by both the relevant budget holder and the owner of the credit card.” (see item 2 from extract above) Two issues were highlighted: • There is not a document called a ‘credit card slip’. A ‘credit card purchase form’ and also a ‘purchase requisition form’ were seen to be used. • There was no evidence that the budget holders had approved expenditure.	The academy should adhere to the processes and approvals within the Financial Procedures Manual. It is advised that the processes within the Financial Procedures Manual are reviewed if required.	
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Medium Priority	The Financial Procedures Manual states "Each credit card holder will need to sign their monthly 'Expense Confirmation Form' from Lloyds once reconciliation is complete to verify that all the expenditure is approved and has been accounted for." (see item 3 from extract above) Four issues were highlighted: • The Lloyds Expense Confirmation Form was not always signed by both the cardholder and the Principal. • The Financial Procedures Manual does not state that the Chair of Trustees should sign the Principal's Lloyds Expense Confirmation Form every month. • The Chair of Trustees was not signing the Principals Lloyds Expense Confirmation Form (it was noted that they do approve individual items of expenditure). • The Lloyds Expense Confirmation Forms for December 2023 could not be located at the time of the review.	The academy should adhere to the processes within the Financial Procedures Manual. The Financial Procedures Manual should include that the Chair of Trustees should approve the Lloyds Expense Confirmation Form for the Principal. Purchase card documentation should be securely stored.	
Management Response:		*Responsibility / Due Date:*	
Medium Priority	The Financial Procedures Manual states "All credit card invoices will be entered onto Sage by the Office Manager (with the support of the PA) and then passed to the SBM for month end reconciliation and signing off." (see item 4 from extract above) At the time of the review it could not be confirmed that month end reconciliation of the purchase card transactions was taking place.	A monthly reconciliation should be undertaken for each purchase card statement to ensure that the finance system reconciles with the statement. Any anomalies should be promptly investigated. The SBM should sign the reconciliations as evidence of the task undertaken.	
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Low Priority	It was noted at the time of the review that some purchase card expenditure items were coded to income codes.	Expenditure items should not be coded to income codes. Having clear and separate income and expenditure codes allows more effective and transparent accounting.	
Management Response:		*Responsibility / Due Date:*	
Low Priority	96 out of 161 transactions (60%) were Amazon transactions. It was advised that the Amazon Business Account is not always used.	Consideration should be given to using the Amazon Business account for all Amazon transactions to enable the academy to have one monthly invoice from Amazon rather than many individual card transactions. This could save significant time and effort on purchase card processes. Consideration should be given to using other business accounts if possible and relevant.	
Management Response:		*Responsibility / Due Date*	

Juniper

RAG	Finding	Recommendation	
Non-Financial Control (Health & Safety)			
Medium	Does the school have the arrangements in place to deal with all serious and imminent danger? **Observation:** The school currently does not have a Business Continuity Plan.	Educational settings should have an emergency plan in place. The plan should explain how you would respond if you needed to take any temporary actions in the event of an emergency. The aim of an emergency plan is to help the school's staff plan for and respond effectively to an emergency. The emergency could happen in the school setting or on an educational visit or outing. Key personnel should be aware of their responsibilities in the event of an emergency.	
Management Response:		*Responsibility / Due Date:*	
Low	First aid supplies are readily available and well stocked? **Observation:** The kitchen first aid box had some out-of-date items.	The school should ensure that items held in the first aid box are within date to ensure suitability for use.	
Management Response:		*Responsibility / Due Date:*	
Low	Are medications stored securely? **Observation:** The medicine cupboard had no lock on the door.	Medicines should be stored securely. Ideally this is in a locked cupboard.	
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Low	Have relevant employees received DSE awareness training/instruction? **Observation:** The Headteacher is responsible for reviewing DSE assessments but has not received DSE specific training.	DSE Specific training will help to review the self-assessments appropriately to ensure all information is being captured and reviewed.	
Management Response:		*Responsibility / Due Date:*	
Low	Have all relevant staff received COSHH training? **Observation:** It was advised that the Site Manager has refresher COSHH training pending.	Ensure all relevant staff carry out COSHH training to help minimise the risks associated with substances used onsite.	
Management Response:		*Responsibility / Due Date:*	
Low	Is someone identified as competent for your premises in relation to Legionella? **Observation:** The legionella duty holder has not received training.	Legionella training empowers you to identify and assess Legionella risk factors specific to your environment. You learn about regulatory requirements and guidelines, enabling you to ensure compliance and implement appropriate preventive measures in between annual risk assessments.	
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Non-Financial Control (Cyber Security)			
	Document in formal written policies how the school approaches cybersecurity. Ensure these policies are aligned across the trust and have been ratified by the board and signed by the board member responsible for cybersecurity. Additionally, secure agreement from the IT service provider to uphold and support these policies.		
Management Response:		*Responsibility / Due Date:*	
	Formally appoint a board member responsible for cybersecurity.		
Management Response:		*Responsibility / Due Date:*	
	Implement cybersecurity as a standing agenda item for the audit and risk committee.		
Management Response:		*Responsibility / Due Date:*	
	Provide regular, accurate and up-to-date information to the board to support their monitoring role in assessing the effectiveness of your school's cybersecurity risk management.		
Management Response:		*Responsibility / Due Date:*	
	Ensure the board allocates and monitors sufficient resources to support cybersecurity initiatives.		
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
	Schedule annual surveillance audits that support this action plan.		
Management Response:		*Responsibility / Due Date:*	
	Create an asset register for information assets (physical, people and data) that details their security requirements, owner, location, encryption status, password status and informs risk assessments.		
Management Response:		*Responsibility / Due Date:*	
	Create flow maps which detail how your data enters and leaves the organisation. These flow maps should encompass the data's origin, storage location, and destination.		
Management Response:		*Responsibility / Due Date:*	
	Create a register (or update the school's information asset register) that identifies or records the school's cloud service providers. This register should also record the service provider's security accreditations, the location of the data and whether data is encrypted in transit and at rest.		
Management Response:		*Responsibility / Due Date:*	
	Revise firewall settings to align with one of the following criteria: a minimum password length of 12 characters with no maximum length, automatic blocking of common passwords with a minimum password length of 8 characters (no maximum length), or the implementation of multi-factor authentication with a minimum password length of 8 characters (no maximum length).		
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
	Revise application/service settings to align with one of the following criteria: throttling the rate of attempts with no more than 10 guesses in 5 minutes or locking accounts after no more than 10 unsuccessful attempts.		
Management Response:		*Responsibility / Due Date:*	
	Maintain documentation of all externally enabled services, including their respective business justifications. Routinely review and disable or delete any services that are no longer necessary.		
Management Response:		*Responsibility / Due Date:*	
	Remove unrequired or unnecessary local user accounts on laptops, computers, servers, tablets, smartphones and cloud services.		
Management Response:		*Responsibility / Due Date:*	
	Remove all software from school devices that is no longer supported by the vendor and, therefore, cannot receive security updates. In cases where there's a business need to use unsupported software, segregate devices with unsupported software into a separate network (or VLAN) and restrict their access to school data and the Internet.		
Management Response:		*Responsibility / Due Date:*	
	Implement a system to manage and monitor the installation of updates to software (including applications and operating systems) installed on devices within 14 days of release and formalise these procedures in written policy.		
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
	Ensure that staff only log into devices and software using a digital identity unique to them.		
Management Response:		*Responsibility / Due Date:*	
	Enable and enforce multi-factor authentication for all accounts that support MFA.		
Management Response:		*Responsibility / Due Date:*	
	Implement a monitoring system to alert administrators of suspected ransomware attacks in motion.		
Management Response:		*Responsibility / Due Date:*	
	Establish a central location for maintaining an audit trail of system and data access by staff across all relevant systems. Implement a regular review process.		
Management Response:		*Responsibility / Due Date:*	
	Develop and implement a formal risk-based process to ensure that all new and modified IT systems including networks, hardware and software applications include the necessary security provisions and adhere to the school's security requirements. This process should be authorised by the board.		
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
	Periodically scan IT systems for known vulnerabilities so that security risks can be treated before being exploited. Report to the board at least annually.		
Management Response:		*Responsibility / Due Date:*	
	Periodically perform penetration tests to measure the effectiveness of already implemented administrative and technical/logic controls. Report to the board at least annually.		
Management Response:		*Responsibility / Due Date:*	
	Establish a formal written cybersecurity incident management plan which includes: - Definition of an incident - How to preserve evidence - Notification of bodies - Roles and responsibilities - Documented lessons learned Run through the formal written cybersecurity incident management plan as a tabletop exercise annually and make necessary plan adjustments based on the exercise outcomes.		
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Non-Financial Control (Site Security)			
Low	Staff conflict resolution awareness training Management could consider providing staff with conflicting resolution/difficult conversation training on a future INSET day. This training should give staff more confidence in dealing with parents who may present challenging behaviour towards staff members.		
Management Response:		*Responsibility / Due Date:*	
Low	Staff awareness Encourage staff to be vigilant regarding parents' parking instead of dropping off or tailgating into the staff carpark and being prepared to politely challenge anyone doing either of the above.		
Management Response:		*Responsibility / Due Date:*	
Low	Staff awareness Encourage staff to be vigilant regarding tailgating into the staff carpark and be prepared to politely challenge anyone doing so.		
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Medium	Conduct a check of boundary fences and overhanging trees It is recommended that any hedging or low hanging tree canopies are trimmed back to reduce the opportunity for trespassers to use these as climbing aids.		
Management Response:		*Responsibility / Due Date:*	
Low	Regular checks of fire escapes It is recommended that fire exits are regularly checked to ensure continued clear egress in the event that a school evacuation is required.		
Management Response:		*Responsibility / Due Date:*	
Low	Consideration for improving cycle security Cycle security could be increased. Consideration could be given to improving security by encouraging parents and pupils to ensure they lock their own property when in the storage facility, through posters and/or briefings in school communications. Consideration could also be given to providing a lockable solution on the storage facility outside of school drop off and pick up times as bikes/scooters can attract opportunist offenders.		
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Low	Alarm system If not already done so, consideration should be given to installing a silent alarm button in reception, linked to the alarm system that would initiate a police response.		
Management Response:		*Responsibility / Due Date:*	
Medium	Improvements to CCTV coverage We recommend the school considers improving the CCTV quality for the rear pedestrian gate by possibly replacing cameras with higher quality resolution/focal length to reach these areas. It is also strongly recommended that a CCTV monitor is installed in the school reception, so staff can monitor main entrances.		
Management Response:		*Responsibility / Due Date:*	
Medium	IT suite security review It is highly recommended that a review of the security of the IT suite/server is undertaken and the cost of additional security measures, balanced against the cost of potential theft of IT equipment.		
Management Response:		*Responsibility / Due Date:*	
Medium	Security of IT equipment Consideration should be given to increasing the security of IT assets that can be easily moved by using cable locks or security cages for example.		
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Medium	Security of tablets or laptops. It is recommended that consideration be given to obtaining a lockable cabinet of security quality that can be bolted to the floor.		
Management Response:		*Responsibility / Due Date:*	
Medium	Consideration to be given on implementing a security marking system. The school maybe advised and assisted in this process by a local Herts Constabulary Crime Prevention Officer (CPO). The local Neighbourhoods Policing Team could possibly advise if there is a CPO and how to contact them.		
Management Response:		*Responsibility / Due Date:*	
Medium	System for managing the issue, return and stock control of keys We recommend that the current system of key control be reviewed as to its suitability. A system where keys are stored and issued, preferably from one location, with an appropriate recording system and overseen by a named person.		
Management Response:		*Responsibility / Due Date:*	
Medium	Additional security controls for managing master keys or those to security sensitive doors It is strongly recommended that suitable and appropriate additional security controls are considered for managing master keys or those to security sensitive doors.		
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Low	Security Policy It is recommended that consideration is given to creating a security policy, which compliments guidance provided by the DfE in their 'Guidance on school and college security ' (2019) https://www.gov.uk/government/publications/school-and-college-security/school-and-college-security.		
Management Response:		*Responsibility / Due Date:*	
Low	Security Policy When considering the implementation of a Security Policy, also consider how it could compliment the existing school safeguarding policy.		
Management Response:		*Responsibility / Due Date:*	
Low	Review of Security arrangements and policy If, on consideration, a security policy is implemented it is recommended that security arrangements, policy and plans are regularly reviewed.		
Management Response:		*Responsibility / Due Date:*	
Low	Site security map It is recommended that the site security map be reviewed to ensure it shows locations of key security features, access points and service isolation points etc.		
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Medium	Staffing of reception throughout the day It is recommended that, if not already implemented, the new office structure to ensure continual staffing of school reception throughout the day is done so as soon as practicable.		
Management Response:		*Responsibility / Due Date:*	
Low	Review of process If not already done, we recommend periodic audits of the visitor management system be conducted to ensure compliance with this policy.		
Management Response:		*Responsibility / Due Date:*	
Medium	Control of delivery drivers access to controlled areas of the site We recommend the current lack delivery drivers access control be reviewed and an appropriate process be implemented.		
Management Response:		*Responsibility / Due Date:*	
Medium	Staff wearing of ID badges or lanyards It is highly recommended that a culture for all staff to wear an ID badge/lanyard is encouraged and non-compliance is challenged. This can enhance the professional image of the school and its staff and also enhance the security of the school, if all non-compliance is politely challenged by all staff.		
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Medium	Wearing of school branded clothing if wearing of ID badges/lanyards is not appropriate It is recommended that a review is conducted to identify all roles where wearing an ID badge/lanyard is not appropriate and ensure these staff members have access to school branded clothing		
Management Response:		*Responsibility / Due Date:*	
Low	In school communication There is already good use of radios to communicate with staff. If not already done so we recommend that consideration is given to the use of for all site staff, duty SMT member and school reception. This will aid communication in a security situation and serves as a deterrent to potential casual offenders.		
Management Response:		*Responsibility / Due Date:*	
Low	External users of the school estate It is good to note that currently the system of electronic signing-in requires acknowledgement of the safeguarding policy. We remind of the importance of closely managing external users due to the potential security risk introduced by familiarity with using the site.		
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Low	Inclusion of Squirrel's Nursery and JAG staff. It is recommended any future security policy should include both the nursery and JAG as they are on the school estate. It is also recommended that a representative from the nursery and JAG should be invited to school Health & Safety meetings.		
Management Response:		*Responsibility / Due Date:*	
Medium	Security emergency procedures Guidance is provided by the DfE in their 'Guidance on school and college security ' (2019). It specifically provides templates for policies, regarding evacuation and 'invacuation' and we recommend the school uses this resource to inform itself, when reviewing its security policy .https://www.gov.uk/government/publications/school-and-college-security/school-and-college-se curity		
Management Response:		*Responsibility / Due Date:*	
High	Lockdown procedure It is highly recommended that the school considers implementing a clear operating procedure for lockdown. In the event of an immediate security incident, initiated by a clear method that is different to that used in the event of fire to enable staff and students to react appropriately and promptly. The use of a different toned alarm to that used for fire and is also recommended that these procedures are communicated with all staff and pupils and practice drills are conducted regularly.		
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Medium	Responding to a bomb threat out hoax A poster of bomb threat procedure is displayed in the reception office. It is recommended that these procedures are incorporated in a new Security policy should the school implement one and all staff made aware of these procedures. Please see my comments above regarding the information and templates available of the DfE website.		
Management Response:		*Responsibility / Due Date:*	
High	Clear and effective procedures for a reported missing child It is highly recommended that clear and effective procedures are introduced for dealing with a pupil reported missing from the site. Advice is contained on the DfE school and college security website. These procedures should be contained within a full security policy.		
Management Response:		*Responsibility / Due Date:*	
Medium	Clear procedures for when and how to call the Police It is highly recommended that clear and effective procedures are introduced for when and how to call the Police as informed by the NPCC's guidance to schools and these procedures should be briefed out to all relevant staff.		
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Low	Emergency 'grab bag' provision It is highly recommended that the school establish a crisis response kit (grab bag) to be secured in reception/Head's office. Further information regarding planning for emergencies can be found on the UK Government website. https://www.gov.uk/government/publications/preparing-for-emergencies/preparing-for-emergencies		
Management Response:		*Responsibility / Due Date:*	
Low	Health & Safety meetings If not already done so, it is recommended that regular Health and Safety meetings include physical security, so any issues raised can be addressed in a timely manner. It is also good practice to minute these meetings with actions raised and how they were addressed, should they be questioned at a later date.		
Management Response:		*Responsibility / Due Date:*	
Medium	Security networks As previously recommended above, consideration should be given to implementing a physical security policy. Without this policy in place, senior staff cannot evaluate or assess the impact any new initiatives may have on its day-to-day operation.		
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Low	External Liaison Consideration could be given to creating a WhatsApp group with other school site managers to share security information especially in real time should there be a security issue locally.		
Management Response:		*Responsibility / Due Date:*	
Low	Access to a named local Pc or PCSO Consideration could be given to being proactive and contacting your local Neighbourhood Policing Team (NPT) and invite them to visit. You could ask for a named contact and suggest that when on patrol in the local area they are welcome to drop by into reception for a chat with staff at any time. Good local informal relations can increase staff and pupils' feeling of safety, if a well-known local officer attends regularly, even if there is no official reason for the visit.		
Management Response:		*Responsibility / Due Date:*	
Medium	Lockdown Procedure As highlighted above consideration should be given to implementing a physical security policy. Within this policy the school lockdown procedures can be specified. It is good practice to carry out these procedures at the start of each term		
Management Response:		*Responsibility / Due Date:*	

Juniper

RAG	Finding	Recommendation	
Medium	Pupil information and training As highlighted above, strong consideration should be given to implementing a physical security policy. Once this policy is in place, pupils can be made familiar with its requirements in an age-appropriate manner.		
Management Response:		*Responsibility / Due Date:*	
Medium	Student information Once a new security policy is documented, it can inform how students can be provided with information and training in an age-appropriate manner about how to react in the event of a knife or firearms terrorist attack.		
Management Response:		*Responsibility / Due Date:*	

Juniper

EMERGING ISSUES

Acquiring and Converting a New School

An education whitepaper published in March 2022, set out the Government's ambition for all schools to be part of a multi-academy trust by 2030. Trusts will be looking to acquire further schools. Juniper can help with the due diligence for this process. Please contact carly.quickcrockford@junipereducation.org should you require any further information.

Wellbeing

It has been reported that staff stress levels are high, leading to many staff leaving the education sector altogether. Mitigating the impact of stress in the workforce should be implemented into everyday trust life by use of a wellbeing charter and strategies and structures that are put in place. Juniper can assess the general wellbeing of staff and provide suitable recommendations to help improve staff wellbeing and staff retention. Please contact carly.quickcrockford@junipereducation.org should you require any further information.

Cyber Security

Cyber security has continued to be a growing area of concern and risk over the past 18 months, with more people working remotely and an increased frequency of email hacking, phishing and malvertising. The July 2020 governance update advises that schools should include an assessment of cyber security within their risk registers, and the ESFA have produced further guidance and suggested questions that trustees can ask on the National Cyber Security Centre website.

GDPR

An increasing number of schools are incurring unplanned costs, both direct and indirect, because of the increase in basic, and easily avoidable, data protection incidents and poorly managed school communications. This is combined with the increasing awareness of data subject of their right to bring a claim [on average in the order of £5,000 per claimant], directly against a school, leading to considerable potential risk to a school. Our GPDR associate has created a briefing video which helps you understand the changing risk to your school and employ some basic strategies and resources to help mitigate them and protect your school against unplanned costs. If you would like access to this briefing, please contact carly.quickcrockford@junipereducation.org

Juniper

USEFUL LINKS

ACADEMY TRUST HANDBOOK

The Academy trust handbook 2023 is effective from September 2023. Trustees should ensure that they have read this document and noted any changes to ensure any new requirements are adhered to.

Academy Trust Handbook 2023 (publishing.service.gov.uk)

INTERNAL SCRUTINY IN ACADEMY TRUSTS

This good practice guide provides guidance for trustees, audit and risk committees, accounting officers, and chief financial officers (CFOs) in academy trusts.

Internal scrutiny in academy trusts - GOV.UK (www.gov.uk)

Bespoke Reviews

If our portfolio of reviews does not include a particular area of interest or risk identified by the trust board, please contact us to discuss our bespoke review options.

Consulting

Juniper is available to provide consulting services in many areas of running a multi academy trust, from centralisation implementation and restructuring to expansion and attracting schools. Please contact us if you would like more information on our consulting work.

Juniper

Non-Financial Reviews Offered

PE & Sports Premium Review

Schools must use PE and sport premium funding to make additional and sustainable improvements to the quality of the PE, physical activity, and sport they provide. Our review will look at whether the funding is being used effectively to develop and add to your provision and examine your own evaluation of the impact using the 5 key indicators set out in the DfE guidance.

Pupil & Recovery Premium Review

Evidence shows that disadvantaged children generally face additional challenges in reaching their potential at school and often do not perform as well as other pupils. Pupil and recovery premium grants provide funding for schools to provide extra support for these pupils. Our review team will take on the role of 'critical friend', highlighting areas of strength around the school's approach to the use of the premiums, but also identifying what can be improved.

Safeguarding Internal Scrutiny Review

Keeping pupils safe is a core responsibility of schools and is rightly a key part of legislation and inspection. A safeguarding internal scrutiny review will assure settings of what they are doing well and provide recommendations to further improve practice and meet and exceed statutory expectations.

SEND Internal Scrutiny Review

Children and young people with special educational needs and disabilities should achieve well in their early years, at school and in college, and lead happy and fulfilled lives. Supporting SEND pupils safe is a core responsibility of schools and is rightly a key part of legislation and inspection. A SEND internal scrutiny review will assure settings of what they are doing well and provide recommendations to further improve practice and meet and exceed statutory expectations.

SEND Ofsted Audit

Though Ofsted doesn't give separate grades for a school's SEND provision, the evidence gathered is used to inform other judgements. Therefore, schools may find it useful to consider their provision in the same way as an inspection might.

We are pleased to offer an audit focussing on Ofsted criteria, in particular the requirements of paragraphs 360 to 364 of the inspection handbook.

Juniper

Sustainability Internal Scrutiny Review

Children and young people should have an understanding of the effects that human use of the world's resources has on them as individuals (including health, wellbeing, and financial wellbeing), the school community, their locality and the world. Our review team will take on the role of 'critical friend', highlighting areas of strength around the sustainability agenda, but also identifying what can be improved.

Teaching & Learning Review

Children and young people's education through the pandemic has suffered. Research is clear that some groups of pupils have fallen further behind than others. A key responsibility of schools is the need to prioritise the teaching of missed content so that pupils will be able to make sense of later work in the curriculum. This includes key knowledge, skills, vocabulary, concepts, and the links between concepts. Our review team will take on the role of 'critical friend', highlighting areas of strength around the school's approach to teaching for education, but also identifying what can be improved.

Juniper