



London Borough of Enfield

Report Title:	Annual School Internal Audit Report 2022-23
Report to:	General Purposes Committee
Date of Meeting:	26 July 2023
Cabinet Member:	Cllr Tim Leaver, Cabinet Member for Finance and Procurement
Directors:	Terry Osborne, Director of Law & Governance
Report Author:	Gemma Young, Head of Internal Audit & Risk Management Gemma.Young@Enfield.gov.uk
Wards affected:	All
Classification:	Part I Public

Purpose of Report

1. This report summarises the findings from school audits undertaken in 2022-23. **Annex A** contains a draft letter due to be sent to the Headteachers, Chairs of Governors and Chairs of Finance/Resources highlighting key statistics and areas for improvement identified during the audits.
2. This letter provides Headteachers and Governors with information on common audit findings which can be used to identify risks in their own schools and helps as a prompt when completing their 2023-24 Schools Financial Value Standard returns for submission to the Department for Education (DfE).

Recommendations

- | |
|---|
| <ol style="list-style-type: none">I. To note the contents on the Annual School Audit Report 2022-23. The report will be shared with Headteachers and Governors at the start of the new academic year. |
|---|

Report Author: Gemma Young
Head of Internal Audit & Risk Management
Gemma.Young@Enfield.gov.uk
Tel: 07900 168938

Appendices

Annex A –Annual School Internal Audit Report 2022-23

Background Papers

None

CE23/003



All Headteachers
All Chairs of Governors
All Chairs of Finance/Resources

Please reply to: Gemma Young

E-mail: gemma.young@enfield.gov.uk

Phone: 07900 168938

Textphone:

Fax:

My Ref:

Your Ref:

Date: July 2023

Dear Headteacher, Chair of Governors and Chair of Finance/Resources

Annual School Internal Audit Report 2022-23

As part of the 2022-23 Internal Audit Plan approved by the Council's General Purposes Committee, Internal Audit carried out 7 full scope governance and financial audits in schools across the borough.

In addition, we conducted a Schools Cyber Security audit and 2 school grant certifications.

Full scope audits

The full scope audits reviewed major processes in schools to ensure:

- compliance with the Scheme for Financing Schools,
- compliance with the Council's Finance Manual for Schools, including the Contract Procedure Rules (CPRs),
- good financial, data security, asset management and business continuity practices were in place.

The Council's school internal audit programme follows the Department for Education's Schools Financial Value Standard (SFVS) headings. The scope areas are detailed in **Appendix 1** and can also be viewed on the School Audit Framework ('Framework') available on the Schools' HUB.

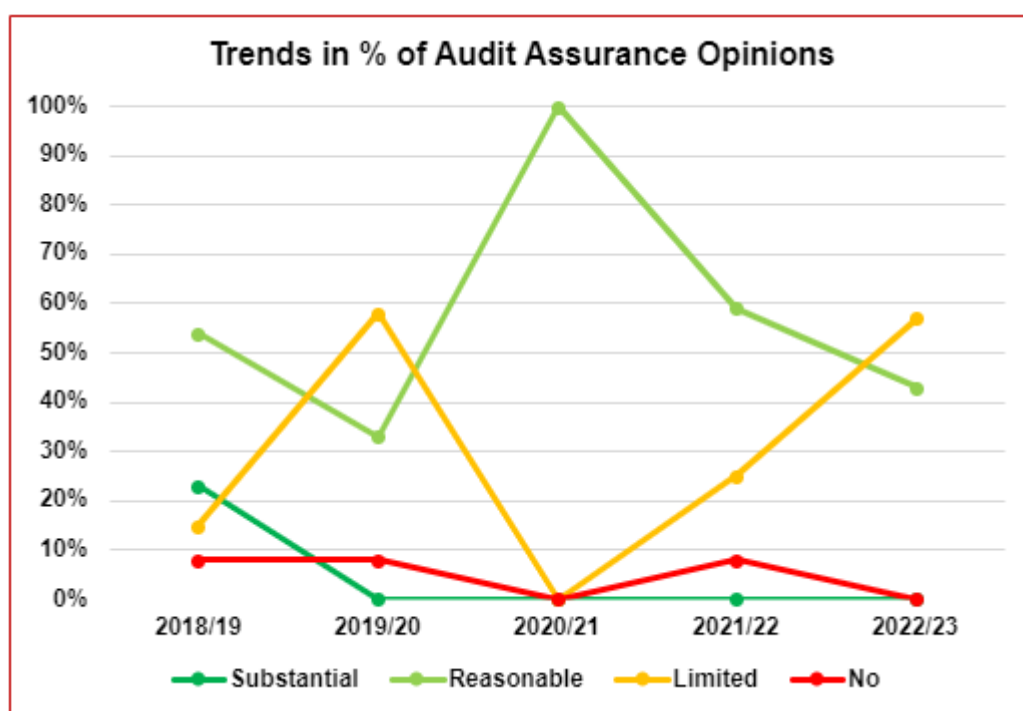
We hope schools continue to find the Framework useful and that School Leadership Teams will use the Annual School Internal Audit Report 2022-23 to identify potential risk areas in their school, or opportunities to make improvements. It may also help as

a prompt when completing the 2023-24 SFVS return for submission to the Department for Education.

The Framework is updated annually to ensure it remains a relevant and useful reference for schools.

Full scope audits - overall report opinions

The trends in assurance opinions over the past five years, are shown in the charts below:



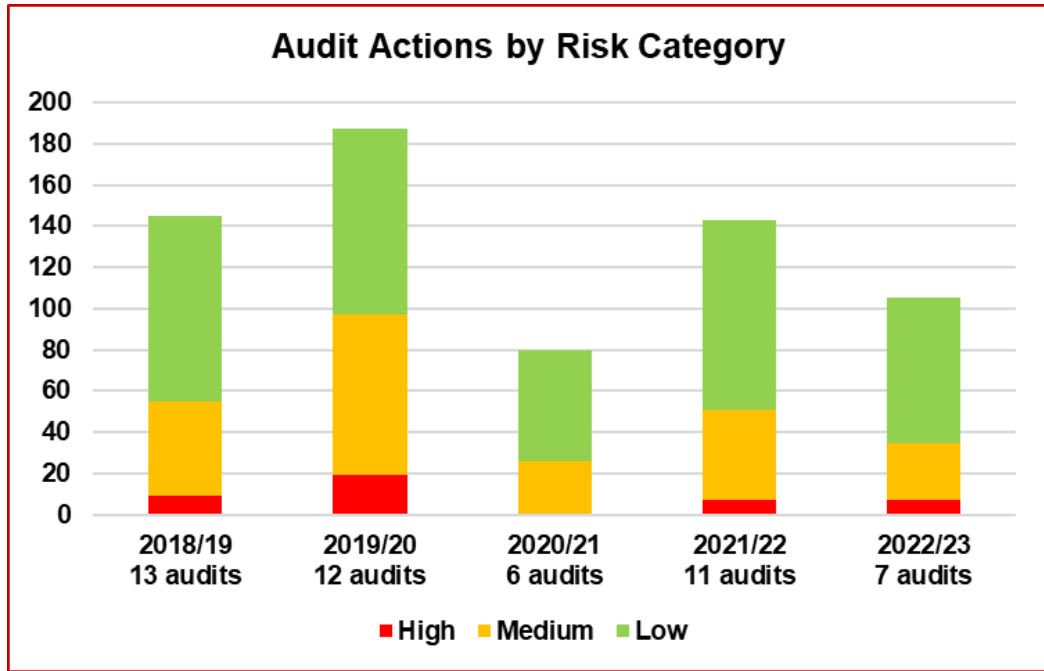
The increase in negative assurance opinions during 2022-23 is a result of weaker controls in the schools tested.

Definitions of risk categories and assurance opinions are detailed in **Appendix 2**.

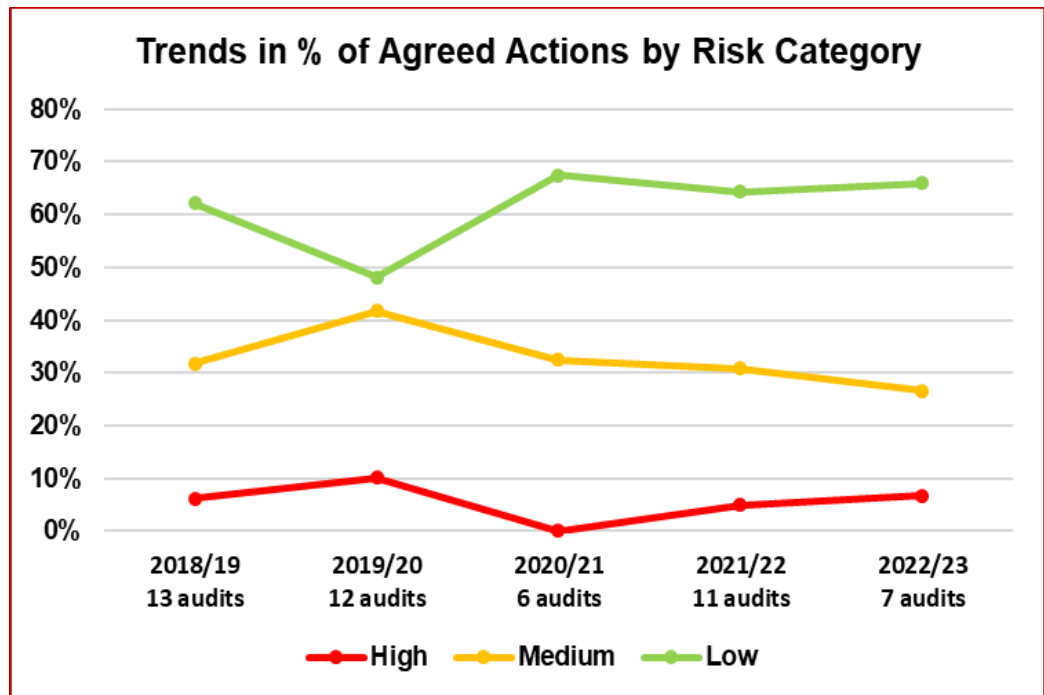
Full scope audits - analysis of actions

As part of our process, actions to address the risks identified by our audits are agreed with Headteachers and School Business Managers. The total number of actions agreed in 2022-23 decreased to 105 from 143 in 2021-22, which is in line with expectations as fewer full scope audits were carried out in 2022-23.

The number of audit actions raised in full scope audits since 2018-19 is shown in the chart below:

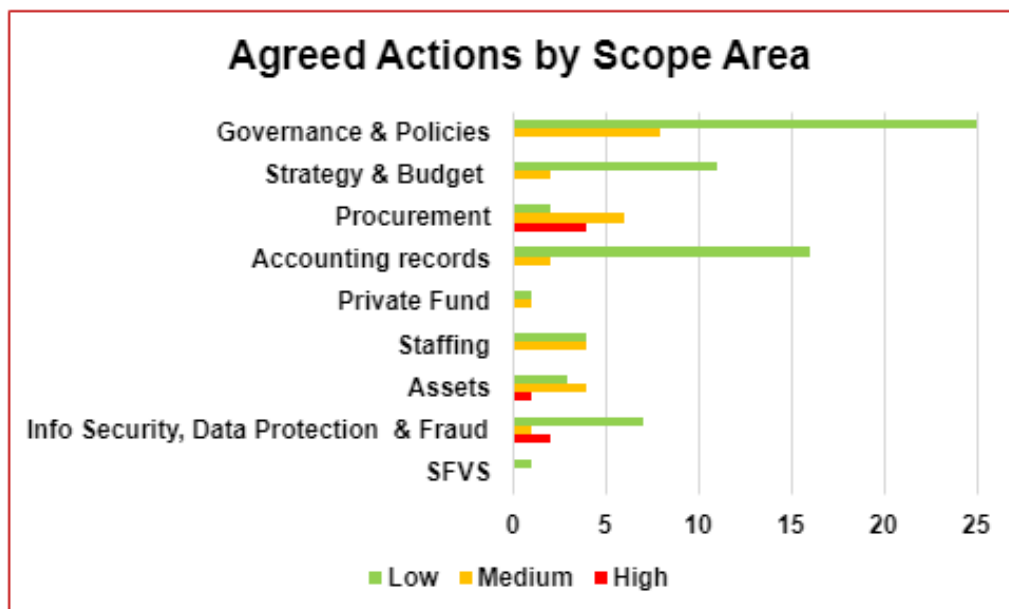


The graph below demonstrates that the proportion of high risk actions agreed is increasing despite the number of audits reducing:



Full scope audits - summary of findings

The chart below summarises the number of agreed actions identified during 2022-23 by scope area:



The main themes and key exceptions identified during our 2022-23 audits are detailed below. We recommend that Governing Bodies review this table against current practices in their schools to ensure, with respect to these common areas, there is compliance with the SFVS requirements.

Theme	Key exceptions identified
Governance	
Business Continuity and Disaster Recovery Plan	<ul style="list-style-type: none"> Disaster recovery plans were either not in place, not approved or regularly reviewed, or were lacking in key details and review dates.
Delegated Authority	<ul style="list-style-type: none"> <i>Organisational Arrangements</i> were not completed fully, were out of date or were still in draft form and not properly approved. <i>Schemes of Delegation (SoD)</i> did not cover all financial responsibilities, including in some cases the BACs payment process, lacked clear segregation of duties for some key financial processes and were not properly approved.
Register of Business Interests	<ul style="list-style-type: none"> Governor business interest forms were not completed or were out of date. Business interest forms had not been completed by staff with financial responsibilities Information published on the school website was out of date
Minutes of Governing Body Meetings	<ul style="list-style-type: none"> Several key decisions were not clearly recorded in Governing Body Meeting Minutes.

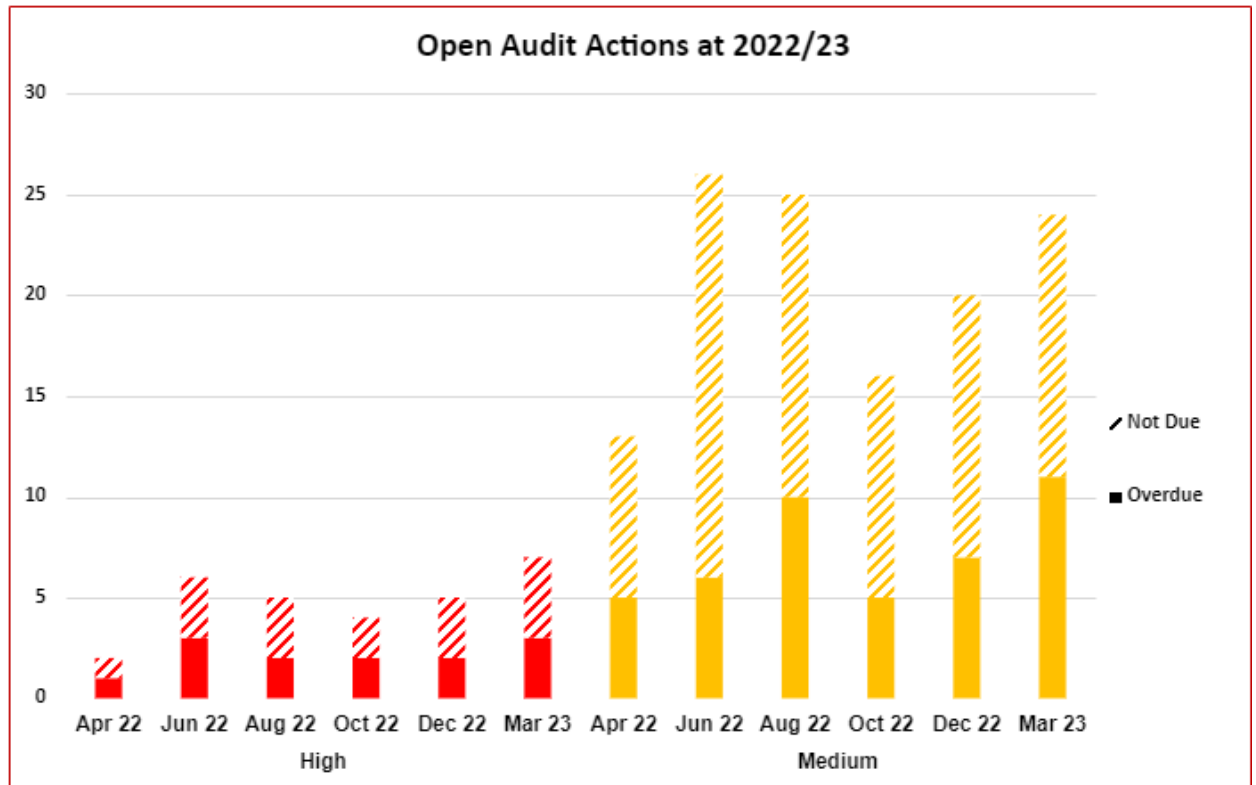
Theme	Key exceptions identified
Policies	<ul style="list-style-type: none"> • Policies that schools are required to have in place had not been reviewed and approved in line with the requirements. • Information that the Department for Education (DfE) requires to be published was not available on the school website.
Strategy & Budget	
Budget Monitoring	<ul style="list-style-type: none"> • We were unable to fully reconcile the quarterly CFR returns to the underlying finance system records.
School Development Plan	<ul style="list-style-type: none"> • The Plan did not cover at least a three year period. • The Plan did not include sufficient financial information to demonstrate that it was aligned to the three year budget.
Staffing Structure	<ul style="list-style-type: none"> • The staffing structure had not been discussed with the governing body in the last 2 years.
Procurement	
Related Party Transactions	<ul style="list-style-type: none"> • Governing Body approval of related party transactions was not recorded in the minutes. • Work was directly awarded without alternative quotes sought to ensure value for money was being achieved.
Contracts	<ul style="list-style-type: none"> • The Council's Contract Procedure Rules had not been adhered to. • Minutes did not reflect that the Governing Body had approved contracts with a value over the Headteacher's delegated limit. • Contracts, signed by both parties, were not in place.
Purchase Testing	<ul style="list-style-type: none"> • Order forms had not been raised or were raised retrospectively. • Order and invoice authorisations were not dated to confirm completion in a timely manner. • Invoices were paid after the due date, with no reasonable explanation noted. • Commercial card transactions were not authorised in advance. • A reconciliation of the commercial card statement to purchases made was not completed and signed.

Theme	Key exceptions identified
Accounting records	
BACs	<ul style="list-style-type: none"> BACs reports were not signed by the required 2 signatories and signatures were not dated to confirm authorised prior to payment. Invoices were approved after BACs payments made
Reconciliations	<ul style="list-style-type: none"> Reconciliations were not completed regularly or where completed there was no evidence of independent review. Unrepresented cheques more than 6 months old were not investigated.
Staff reimbursements	<ul style="list-style-type: none"> A large float was issued to a member of staff, but no receipts or invoices were supplied with the returned balance to support expenditure incurred. Claim vouchers were not properly completed. High value items were reimbursed, but these items should have been purchased through the school's usual purchasing processes.
Lettings	<ul style="list-style-type: none"> No signed agreements were in place for long-term and ad hoc lets. We could not confirm appropriate insurance arrangements were in place. Agreements were not signed by the school's delegated officer(s).
Private fund	
Accounting records	<ul style="list-style-type: none"> An annual audit had not been completed and approved by the governing body.
Staffing	
Starters and leavers	<ul style="list-style-type: none"> Pre-employment checks were not completed in full prior to employment commencing. There was no written evidence of who had carried out and verified pre-employment checks. Videpay forms for leavers and starters were not supplied to the Schools Personnel Service in sufficient time to ensure necessary action could be taken.
Additional hour claims	<ul style="list-style-type: none"> Additional hours claim forms were not completed in full,

Theme	Key exceptions identified
	totalled correctly nor appropriately authorised and dated.
Assets	
Fixed Assets	<ul style="list-style-type: none"> • Assets were recorded in two different systems, which did not interface, with inconsistencies in the information recorded in each. • A list of IT equipment collected by a disposal company was not retained so we could not that all items had been disposed of appropriately. • The fixed asset register did not capture key information including acquisition dates, purchase costs or disposal details. • There was no evidence that annual fixed assets checks had been carried out. • Formal records were not kept or were not updated of assets loaned to staff. • Assets were not appropriately security marked.
Information Security, GDPR & Fraud	
Physical and data security	<ul style="list-style-type: none"> • Records of fob access to the school were poorly maintained. • A high number of anomalies were identified between records of fob access and management information system access when compared to staff lists. • No process or mechanism was in place to prevent staff from using unencrypted removable media on school equipment. • There was no requirement to ensure passwords were changed regularly or had sufficient complexity.

Full scope audits - action implementation

Schools have continued to make progress on action implementation. Progress made is shown in the following chart:



The Council takes the implementation of internal audit actions seriously and overdue actions are reported to both the Assurance Board and the General Purposes Committee.

Therefore we follow up with schools to confirm that all actions are implemented within the agreed target dates. Also:

- findings from the internal audit reports given a Limited or No assurance opinion are reported to the Assurance Board and the Council's General Purposes Committee.
- follow up emails and/or visits are undertaken in accordance with the target dates agreed within the report.
- if timely and appropriate responses are not received, this is escalated to the Audit and Risk Manager and if necessary, to the Director of Education.
- if it is deemed that sufficient responses have not been received, and/or satisfactory progress has not been made, the Director of Education is informed. Actions taken are reported to the Assurance Board.

The Director of Education also considers whether the Headteacher and/or the Chair of Governors should attend the Assurance Board. Attendance would be to advise the Assurance Board of action being taken to address the findings.

Schools Cyber Security audit

Due to the nature of the audit (a questionnaire sent to the 55 maintained schools), we did not form an audit opinion and instead issued a management letter outlining our findings. The management letter has been shared with all Headteachers and has been referenced in the Summer Termly Pack for Governors

The audit was designed to assess the schools' knowledge of, and ability to avoid, identify, or respond to a cyber-attack. The questionnaire was based on:

- the Department for Education standards on schools' cyber security, user accounts and data protection; and
- the National Cyber Security Centre Cyber Essentials

The questionnaire covered:

- security measures currently in place
- cyber security training undertaken
- any cyber-attacks/ breaches experienced
- cyber security concerns generally

We received 54 completed surveys, a response rate of 98%.

A number of concerning control weaknesses were identified. This poses a risk not only to individual schools, but also to the wider Council network given the digital links, close working and constant communication between schools and Council services.

The key findings were:

- 87% of schools had not undertaken phishing attack exercises
- 84% of schools did not have a Data Governance and Cyber Security Risk Register in place
- 61% of schools did not give regular updates to the governing body and believed the governing body did not understand the current state of cyber security awareness in the school
- 46% of schools did not conduct any cyber training for staff
- 43% of schools did not feel adequately prepared in the event of a cyber attack
- 48% of schools did not have a Business Continuity and Disaster Recovery Plan in place
- 30% of schools did not have an IT Cyber Security policy or plan in place

We also noted that 12% of schools had experienced a malware infection including viruses or ransomware.

We recommend that each school:

1. presents and discusses the report at a governing body meeting.

2. reviews their own arrangements against:
 - The Department for Education standards on schools' cyber security, user accounts and data protection; and
 - The National Cyber Security Centre Cyber Essentials.
3. develops an action plan for improvement that is monitored regularly by the governing body.

The full Schools Cyber Security report can be found at **Appendix 3**.

Training

We offer audit and fraud training for both Governors and School Business Managers. The training includes an overview of the Council's Internal Audit and Counter Fraud services. Training is delivered by experienced officers and provides:

- an overview of internal audit scope areas
- the importance of good controls
- key fraud risks faced by schools, with a particular focus on cybercrime.

Further information can be found on the Schools' HUB.

Acknowledgement

We would like to take this opportunity to thank those schools who were included in the 2022-23 internal audit programme. We recognise the additional work and effort involved during an internal audit and the support of you and your teams in ensuring the process runs smoothly is appreciated.

Should you have any comments on this report, require further clarification, or wish to raise any concerns, the Internal Audit team would be happy to discuss these with you (please see below for contact details).

Yours sincerely,

Gemma Young
Head of Internal Audit and Risk Management



APPENDIX 1 – Internal Audit Scope Areas

Scope area:	To ensure that:
Governance	<ul style="list-style-type: none"> • Appropriate Governance structures are in place; are appropriately resourced; and operate in line with Council regulations and best practice. • Relevant policies are in place; are reviewed and up to date; and are available on the school’s website. Website content complies with DfE requirements. • The school has up to date business continuity and disaster recovery plans in place.
Strategy and Budget	<ul style="list-style-type: none"> • The school has a realistic, sustainable and flexible financial strategy in place for at least the next 3 years which has a demonstrable link to the school development plan. • The school sets a well-informed and balanced budget each year and this budget is scrutinised and approved by the Governing Body. The budget includes realistic assumptions and can be flexed if required. • Performance against budget is monitored throughout the year; variances are investigated; and remedial actions are taken where necessary.
Procurement	<ul style="list-style-type: none"> • All expenditure incurred: <ul style="list-style-type: none"> ○ Is necessary for the running of the school; ○ Complies with the Council’s Finance Manual for Schools’ and the Council’s Contract Procedure Rules (CPRs); and ○ Is appropriately authorised and is supported by appropriate documentation.
Accounting Records	<ul style="list-style-type: none"> • All transactions are authorised and are supported by appropriate documentation. • Regular reconciliations are made between the accounting records and supporting information. • Payments are made within agreed timescales; are made in line with policy; and are appropriately authorised. • All adjustments to the financial records are appropriately recorded and authorised. • VAT is appropriately accounted for.

Scope area:	To ensure that:
	<ul style="list-style-type: none"> • Income is fully accounted for and is banked promptly. • Debts are reviewed to ensure t payment is received promptly.
Private Fund	<ul style="list-style-type: none"> • The standard for the governance of the private fund is as rigorous as that for the administration of the school's delegated budget and complies with the Council's Finance Manual for Schools
Staffing	<ul style="list-style-type: none"> • The school reviews and challenges its staffing structure regularly to ensure it is the best structure to meet the needs of the school whilst maintaining financial integrity. • Staff are adequately vetted to ensure their suitability for employment. • Payments to permanent, supply and agency staff are valid and are appropriately authorised. • IR35 assessments are carried out as necessary.
Assets	<ul style="list-style-type: none"> • Fixed assets and stock are properly accounted for; are kept securely; and are periodically checked for existence and condition.
Information Security, GDPR and Fraud	<ul style="list-style-type: none"> • Access to the school's systems and data is well controlled. • The school complies with GDPR legislation and best practice. • All appropriate steps are taken to reduce the likelihood of fraud.
SVFS and Risk Assessment Returns	<ul style="list-style-type: none"> • The Governing Body has approved the final checklist and dashboard. • Follow up actions have been identified and actioned. • Approved returns are submitted to the Council by the required deadlines.

APPENDIX 2 - Definition of Risk and Assurance Ratings

Risk rating	
<p>Critical</p> <p>●</p>	<p>Life threatening or multiple serious injuries or prolonged workplace stress. Severe impact on morale & service performance. Mass strike actions etc.</p> <p>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.</p> <p>Cessation of core activities, Strategies not consistent with government's agenda, trends show service is degraded. Failure of major Projects – elected Members & SMBs are required to intervene</p> <p>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</p>
<p>High</p> <p>●</p>	<p>Serious injuries or stressful experience requiring medical many workdays lost. Major impact on morale & performance of staff.</p> <p>Significant impact on the reputation or brand of the organisation; Scrutiny required by external agencies, Audit Commission etc. Unfavourable external media coverage. Noticeable impact on public opinion</p> <p>Significant disruption of core activities. Key targets missed; some services compromised. Management action required to overcome med – term difficulties High financial loss Significant increase on project budget/cost. Service budgets exceeded. Significant breach in laws and regulations resulting in significant fines and consequences</p>
<p>Medium</p> <p>●</p>	<p>Injuries or stress level requiring some medical treatment, potentially some workdays lost. Some impact on morale & performance of staff.</p> <p>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.</p> <p>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.</p>




	Medium financial loss - Small increase on project budget/cost. Handled within the team. Moderate breach in laws and regulations resulting in fines and consequences
Low 	<p>Minor injuries or stress with no workdays lost or minimal medical treatment. No impact on staff morale</p> <p>Internal Review, unlikely to have impact on the corporate image. Minor impact on the reputation of the organisation</p> <p>Minor errors in systems/operations or processes requiring action or minor delay without impact on overall schedule. Handled within normal day to day routines.</p> <p>Minimal financial loss – Minimal effect on project budget/cost. Minor breach in laws and regulations with limited consequences</p>
Advisory 	Advisory findings or observation that would help to improve the system or process being reviewed or align it to good practice seen elsewhere.

Level of assurance

Substantial



No significant improvements are required. There is a sound control environment with risks to key service objectives being well managed. Any deficiencies identified are not cause for major concern.

Reasonable 	Scope for improvement in existing arrangements has been identified and action is required to enhance the likelihood that business objectives will be achieved.
Limited 	The achievement of business objectives is threatened and action to improve the adequacy and effectiveness of the risk management, control, and governance arrangements is required. Failure to act may result in error, fraud, loss or reputational damage.
No 	There is a fundamental risk that business objectives will not be achieved, and urgent action is required to improve the control environment. Failure to act is likely to result in error, fraud, loss or reputational damage.

APPENDIX 3 – Schools Cyber Security Internal Audit

Internal Audit of Cyber Security in Schools

This review was undertaken as part of the 2022-23 Internal Audit programme agreed by the Council's General Purposes Committee.

Background

A Cyber Security Breaches survey (2022) conducted by the Department for Digital, Culture, Media & Sport (DCMS) found 41% of primary schools and 70% of secondary schools surveyed had identified cyber breaches or attacks during 2021-2022. Secondary schools saw a significant increase in identified breaches or attacks in 2022 over 2021 with 70% reporting breaches in 2022 compared to 58% in 2021.

Schools hold a substantial amount of personal, and often sensitive, data on their staff, pupils and their families. They may also hold information on behalf of volunteers, contractors and other partners. Schools also have key digital links with many Council departments. In a climate of pressured budgets, schools may not always consider cyber security as a priority when faced with challenging budget choices for safeguarding, staffing and academic achievement.

The purpose of this review was to understand the current position in Council maintained schools in Enfield ('maintained schools') with regards to the cyber security preparedness.

Objectives, approach, and scope

The audit was designed to assess the current understanding of maintained schools regarding their knowledge of, and ability to avoid, identify, or respond to a cyber-attack.

A Microsoft Forms survey was issued to all 55 maintained schools to cover:

- Security measures currently in place
- Cyber security training undertaken by the school
- Any cyber-attacks/ breaches the school has experienced
- Cyber security concerns the school has.

Executive Summary

We received 54 completed surveys, a response rate of 98%.

The key findings were:

- 87% of schools had not undertaken phishing attack exercises
- 84% of schools did not have a Data Governance and Cyber Security Risk Register in place

- 61% of schools did not give regular updates to the Governing Body and believed the Governing Body did not understand the current state of cyber security awareness in the school
- 48% of schools did not have a Business Continuity and Disaster Recovery Plan in place
- 46% of schools did not conduct any cyber training for staff
- 43% of schools did not feel adequately prepared in the event of a cyber attack
- 30% of schools did not have an IT Cyber Security policy or plan in place
- 12% of schools had experienced a malware infection including viruses or ransomware.

A summary of all responses received can be found in **Appendix A**.

Conclusion

There are a number of concerning control weaknesses in schools around cyber security. This poses a risk not only to individual schools, but also to the wider Council network given the digital links, close working and constant communication between schools and Council services.

Every school leadership team has a responsibility to ensure their school has robust cyber security measures in place. This report is being shared with all headteachers and governing bodies to highlight areas of concern and to act as tool for reviewing circumstances in their own school.

Recommendations

1. Each school should present and discuss this report at a governing body meeting.
2. Each school should review their own arrangements against:
 - the Department for Education standards on schools' cyber security, user accounts and data protection; and
 - The National Cyber Security Centre Cyber Essentials

Following these actions, an action plan for improvements should be developed and monitored regularly by each school's governing body. We will follow up that these actions have been taken as part of our schools Internal Audit programme.

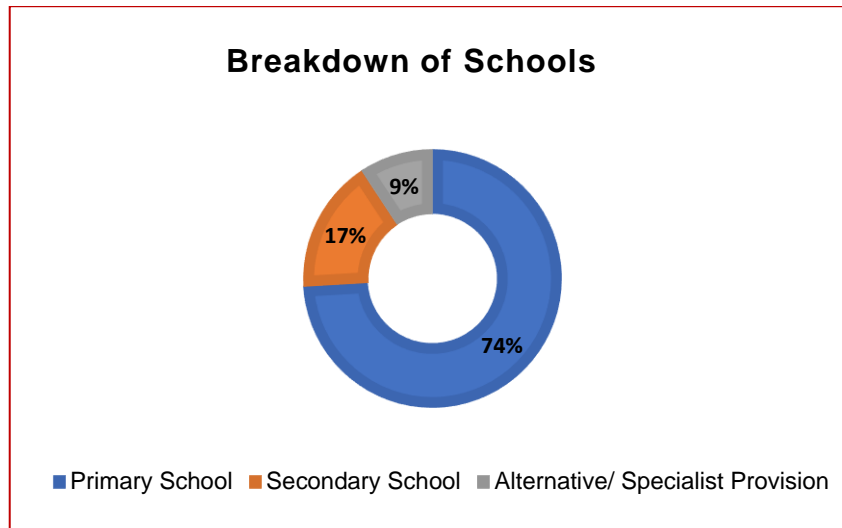
Additional sources of information and advice can be found in **Appendix B** and a glossary of terms can be found in **Appendix C**.

Appendix A – Survey Results

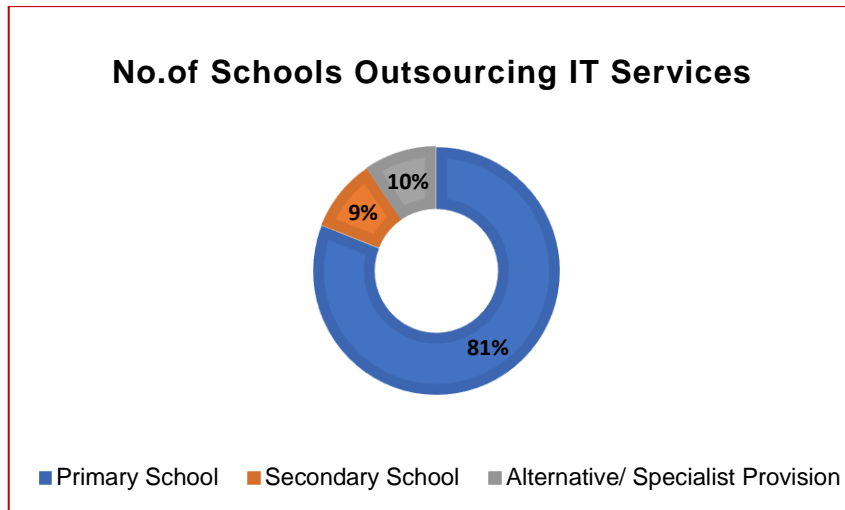
The survey was sent to all 55 maintained schools. Responses were received from 54 schools.

1. Breakdown of responses received

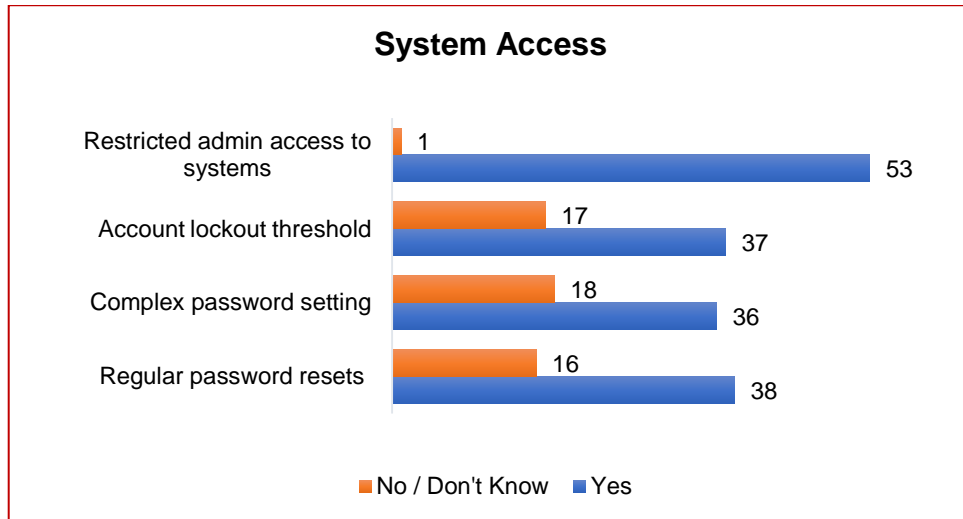
a) Number of schools who completed the Survey



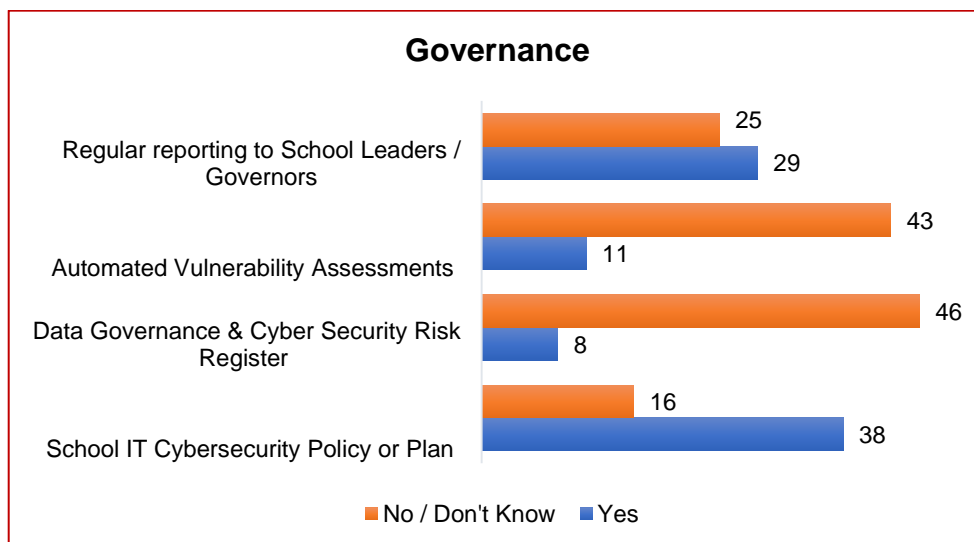
b) Of these 54 schools, 42 outsourced their IT services



2. School Cyber Security Measures



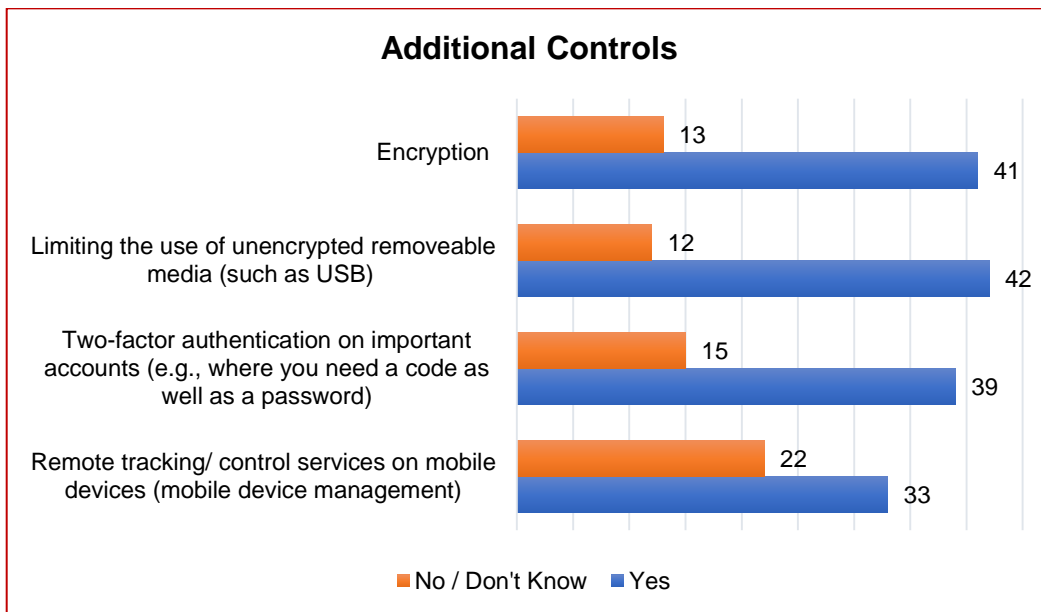
- Most schools had restricted admin access to systems
- 50% of the schools who did not carry out regular password resets, also did not enforce complex password settings.



Most schools had some governance security measures in place. However, the areas of concern included:

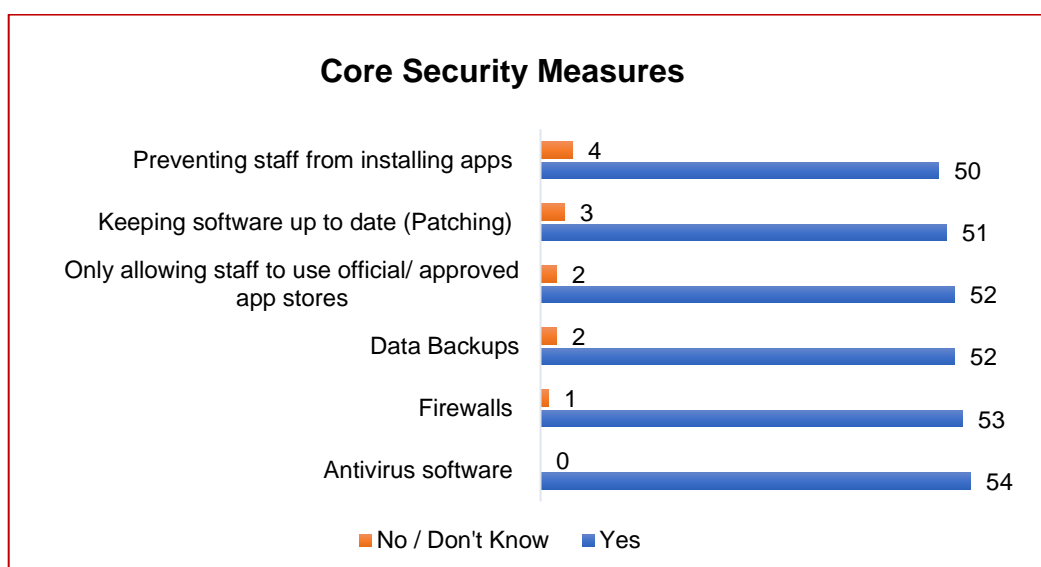
- 85% of schools did not have a Data Governance and Cyber Security risk register

- 80% of schools had not undertaken an automated vulnerability assessment
- 46% of schools did not provide regular reporting to school leaders / governors



We noted that:

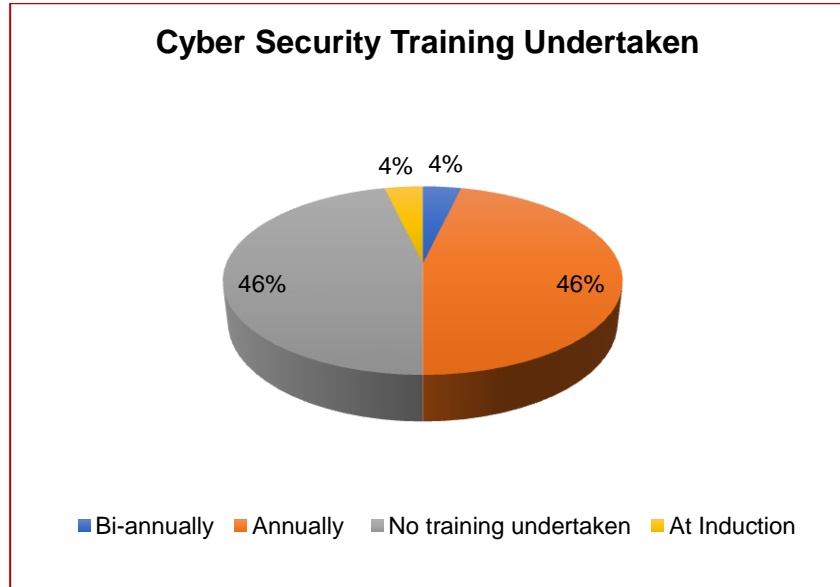
- 24% of schools did not encrypt their data
- 22% of schools did not limit the use of unencrypted removable media (such as USB and/or memory cards)
- 28% of schools did not have two-factor authentication on important accounts
- 41% of schools did not control services on mobile devices/ device management



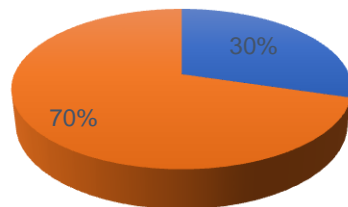
Although most schools had these core security measures in place, there was a minority of schools who did not prevent staff from installing apps onto school devices, keep software up to date, allow staff to only use official or approved app stores, or backup data.

3. Cyber Security Training

46% of schools did not require staff to undertake any cyber security training.



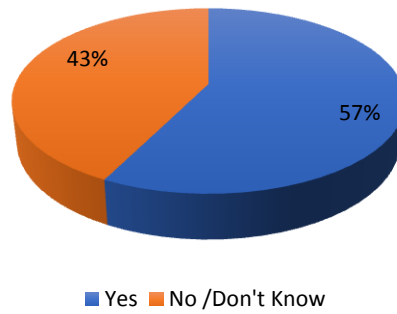
Requires all staff to complete Cyber Security training at the point employment commences



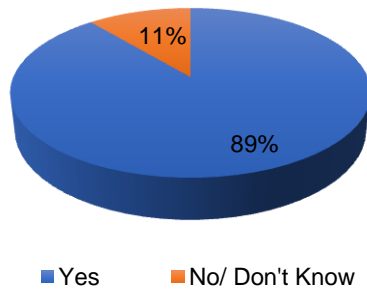
70% of schools did not require staff to complete cyber security training at the point employment commenced.

43% of schools did not feel adequately prepared in the event of a cyber incident

Do you feel the school is adequately prepared in the event of a cybercrime ?



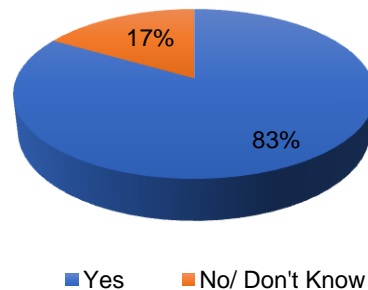
In the event of a data breach, do you know what to do ?



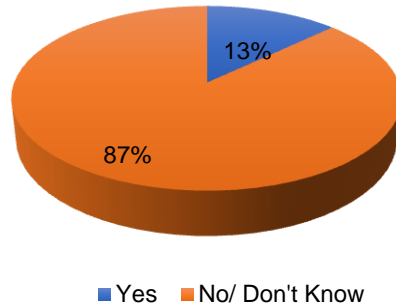
11% of schools said they did not feel that they would know what to do in the event of a data breach

17% of schools said they did not know who to contact in the event of a cyber incident such as a virus or ransomware attack

In the event of a cyber incident such as a virus or ransomware attack, do you know who to contact



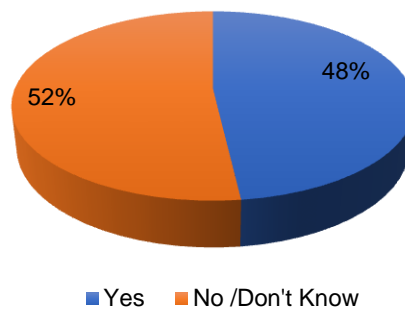
Has your school undertaken a phishing attack exercise to test robustness of cyber security measures ?



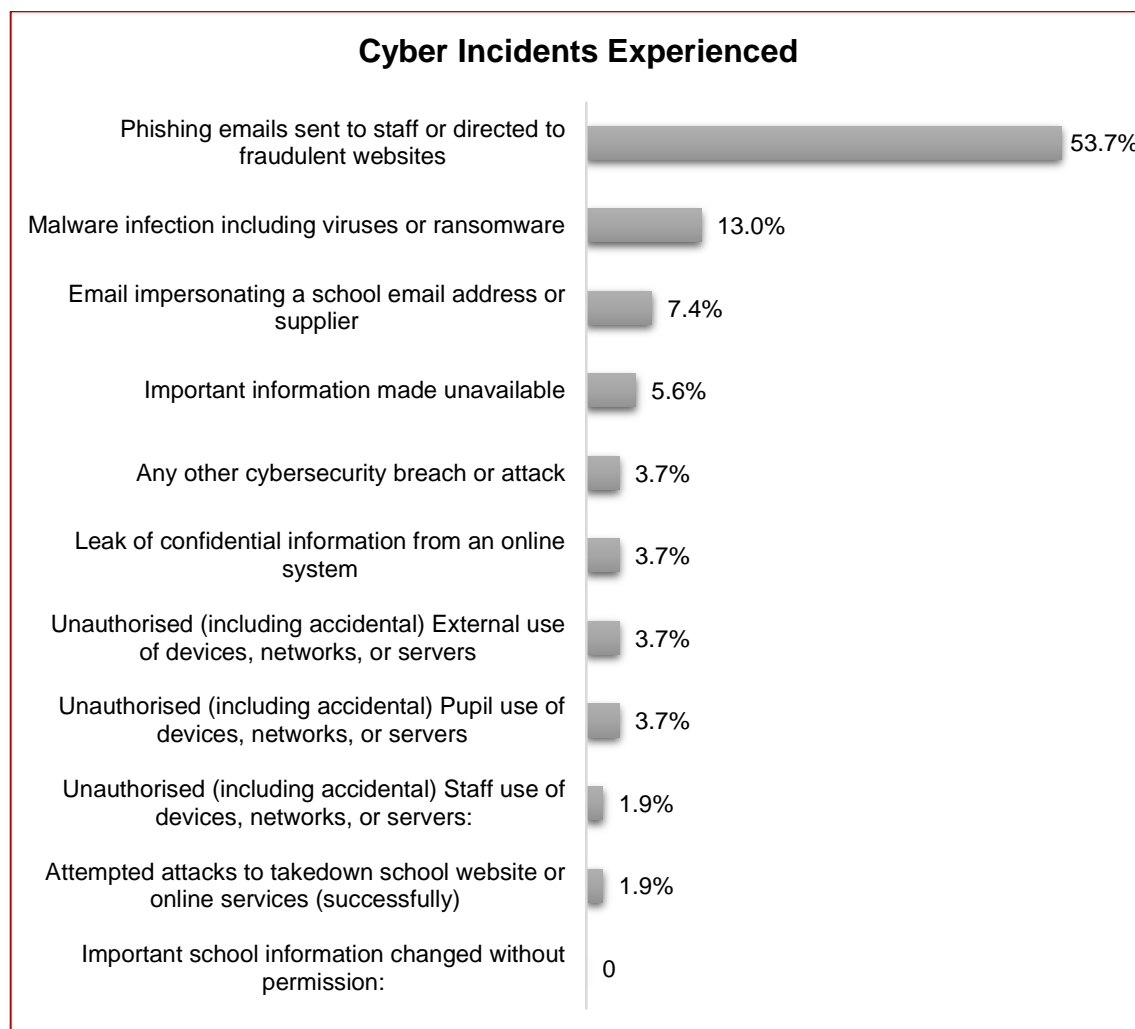
87% of schools had not undertaken a phishing attack exercise to test robustness of cyber security measures

52% of schools were unaware that the National Cyber Security (NCSC) offered free cyber security training to schools. Of the 48% of those schools that were aware of this training, 65% had not taken advantage of this

Awareness of National Cyber Security Centre (NCSC) free cyber security training for schools

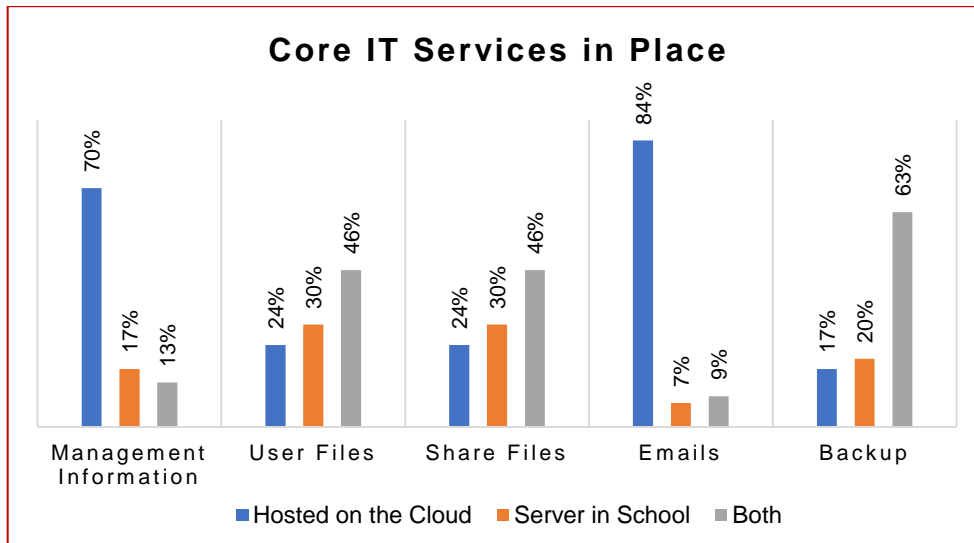


4. Breakdown of incidents experienced by schools



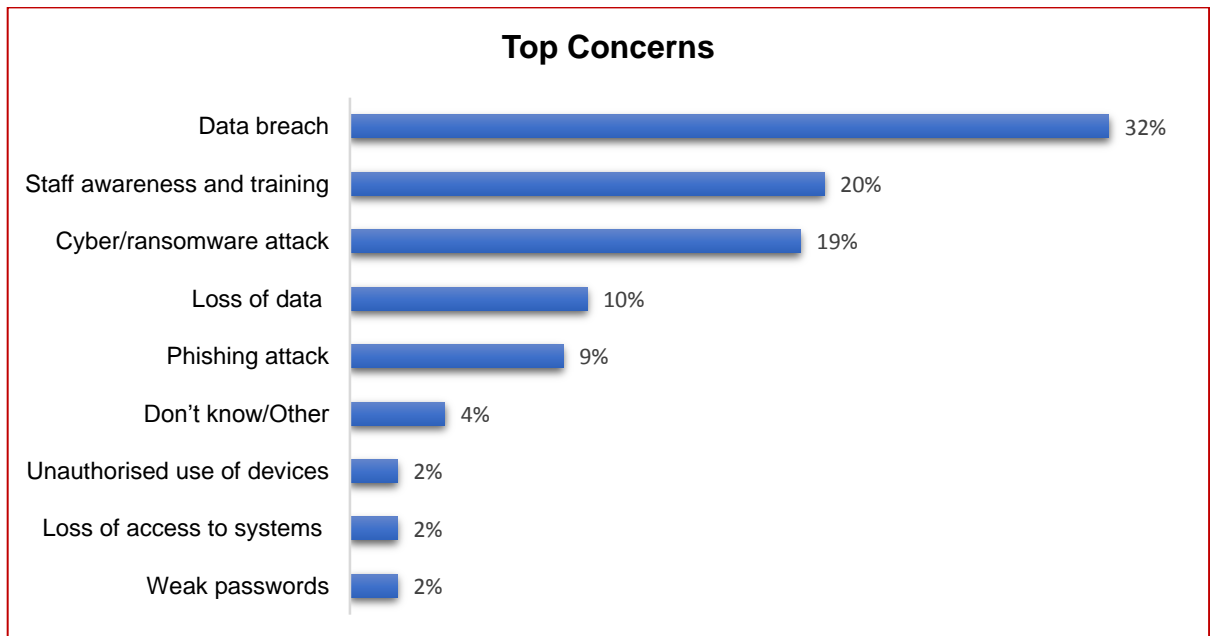
- 29 of the 54 schools had received a phishing email sent to staff, or directed to a fraudulent website
- 7 schools had experienced a malware infection including a virus or ransomware; 6 of these were also a target of phishing.
- 4 schools received an email impersonating a school's email address or supplier.
- 3 schools had experienced important information being made unavailable as a result of a cyber incident.

5. Breakdown of Core IT Services



- 70% of schools management information systems were hosted on the cloud; 80% of schools also hosted emails on the cloud
- 63% of schools hosted backups on both the cloud and the school server

6. Schools' Concerns



7. Government Risk Protection Assurance

We understand that a number of schools are insured through the Government's RPA scheme which includes emergency assistance in the event of a cyber incident. These schools should be aware that in the event of a claim the school must be able to evidence the following conditions:

- Offline backups are in place and are tested appropriately to ensure data can be recovered
- All employees or governors who have access to the management information technology system must undertake National Cyber Security Centre training.
- The school is registered with Police CyberAlarm
- The school has a Cyber Response Plan in place.

Appendix B – Useful Links

For further information, help and support to help improve cyber security arrangements in your school:

- **DFE- Digital and Technological Standards**

<https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges>

- **Cyber Essentials – National Cyber Security Centre**

<https://www.ncsc.gov.uk/cyberessentials/overview>

- **The National Cyber Security Centre**

<https://www.ncsc.gov.uk/>

- **London Grid for Learning CyberSafe**

<https://www.lgfl.net/learning-resources/summary-page/cybersafe>

- **Government’s Risk Protection Arrangement (RPA)**

For schools insured with the Risk Protection Arrangement (RPA)
<https://therga.org.uk/wp-content/uploads/2022/04/RPA-Cyber-Guidance.pdf>

- **Enfield Council Digital Services Security Team**

DSSecurity@Enfield.gov.uk

Appendix C – Glossary

Antivirus

A software designed to detect, prevent, and remove viruses, malicious software, and viruses.

Allowed List

An authorised approved list of applications for use to protect systems from potentially harmful applications.

Automated Vulnerability Assessment

Automated processes of detecting defects in an organisation's security

Breach

An incident where data, applications, computer networks or systems are accessed or affected in a non-authorised way.

Cloud

Shared resources are available to be accessed remotely through the internet.

Cyber Attack

Any kind of malicious attempt to collect, damage, disrupt, destroy or gain unauthorised access to computer systems, networks or devices.

Cyber Incident

A breach of a system's security policy in order to affect its integrity or availability and/ or the unauthorised access or attempt access to a system or systems.

Cyber Security

The process of protecting information by preventing, detecting, and responding to attacks.

Encryption

A function that protects information by making it unreadable by everyone except those with the key to decode it.

Firewall

Hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorised access to or from a network.

Malware

A malicious software that includes viruses, trojans, worms, or any code or content that could have an adverse impact on organisations or individuals.

Network

A group of two or more computers or other electronic devices that are interconnected for the purpose of exchanging data or resources.

Patching

Applying updates to firmware or software to improve the security and or enhance functionality

Phishing

Mass emails sent to users requesting sensitive information or encouraging them to visit fake websites.

Ransomware

A malicious software used to prevent users from accessing data or systems usually by encryption, in exchange for a payment.