MOORE Kingston Smith

Academies Plus (A+)

April 2024

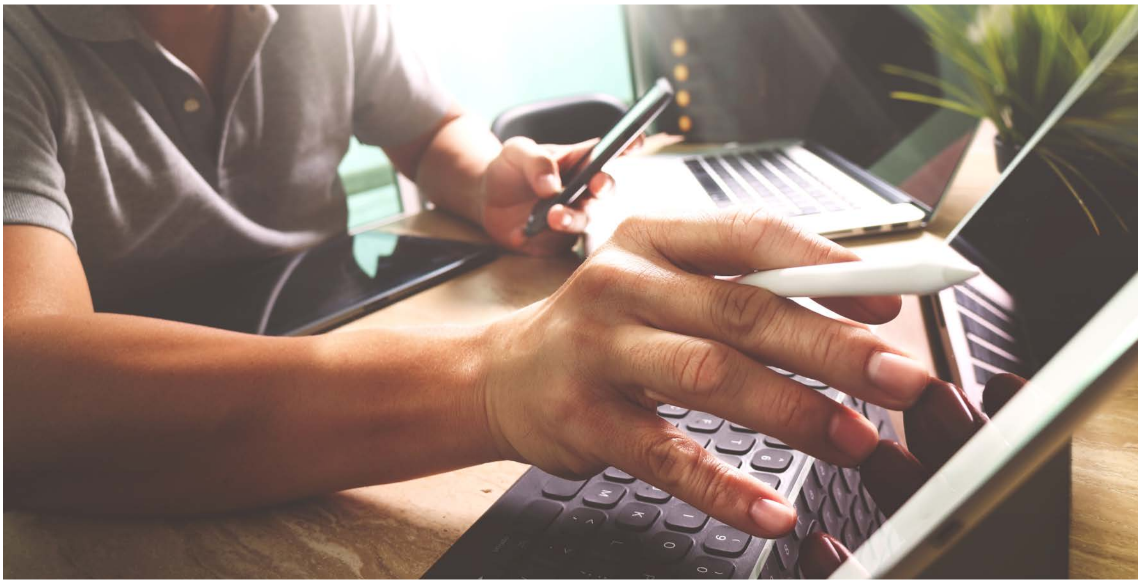
Contents

Client perspectives - Voices from the frontlines

By James Saunders, Head of Academies, Moore Kingston Smith

The fast-evolving world of academy trusts continues to throw up new challenges and new slants on existing challenges – our clients and contacts are telling us about the following issues they are currently grappling with:

- Reinforced Autoclaved Aerated Concrete – or the dreaded acronym "RAAC". The crisis of Autumn 2023 continues to impact on many schools who even now remain away from buildings that overnight become unexpectedly classed as dangerous. The impact on pupils and finances is, and will continue to be, significant to a number of trusts and the full implications really have yet to be judged. Reported at the end of March 2024, it has become apparent that the Department for Education's (DfE) school improvement budgets have been absorbed by RAAC-related remedial work at the expense of many other worthy cases, meaning that even more schools that are in desperate need of money for capital projects will have been bumped down or off the list.
- Tension over top slicing – the recent case of a school head resigning because of disagreements over budgets is unlikely to be an isolated incident of tension concerning centralised management of individual school budgets. In our experience, GAG Pooling and Top Slicing can be divisive if implemented, managed, and generally handled badly – equally (and generally more often) it can be a fair and acceptable way of recognising centralised efficiencies if implemented in an engaging, collaborative and sympathetic manner. But it is an enormously difficult and delicate matter to get right, and really speaks to the culture of a MAT and its constituent parts.
- School meals trauma – another very recent high profile news story has highlighted not just the occasional



disparities between what school catering companies claim to serve up and what they actually provide, but also how difficult it is for relatively small educational establishments to deal with such large national organisations who operate on such a wide landscape. In the interests of fairness, it should be said that there are of course cost pressures on the catering companies that must be very difficult to manage (although that is most definitely not meant to excuse the standard of provision served up). School meal budgets will inherently go further in the bigger organisations – smaller organisations such as stand-alone academy trusts will no doubt find this to be even more of a challenge in the next few months and years as budgets are being formulated, and need to be aware that costs are only going one way.

- Ofsted is back - and anecdotally the inspectors have been inconsistent on their return to the fray. I have heard commentary that visits have been carried out with a noticeably less hostile demeanour - and equally some remain punchy. Clearly there is a balance to be struck going forwards between the demands of the regulator's role and the excessively aggressive attitude of the recent past – but the biggest challenge for Ofsted itself may well be to be consistent in their approach given they will undoubtedly be under the microscope in the coming months.
- Safeguarding iterations - safeguarding is undergoing its regular ongoing natural evolution and also dealing with fast-changing new challenges around transgender policies, guidance, and regulations. This is another topic which garners high media attention and individual cases can go viral from the most unexpected beginnings. All schools and trusts must be very aware of the risks they face when taking on any issues in this area, and ongoing training (both formal HR and softer awareness education) is vital around these matters.
- Cyber warfare – the threats of cybercrime continue to evolve and for every safeguard that is put in place, it will only be a matter of weeks (if not days) before the cyber hackers get one step ahead and manage to scam a new innocent party out of public money. We cannot say it often or loudly enough: **the charity sector, and particularly the education sector, and even more the academy sector, are seen as soft targets by cyber criminals.** This is a combination of perceived weak security, the prevalence of personal and sensitive data about children (which attracts a higher ransom value), and the interconnection of disperse schools' systems (which open abnormally high levels of access to hackers), all of which mean that the education sector is currently one of the most-targeted sectors by hackers in the UK.
- Change in government – wherever you sit on the political spectrum, the result of the upcoming UK General Election (expected to be in the autumn this year) is sadly unlikely to provide a revolution in funding to any public sector. Right now, there simply isn't the right balance of government money and public needs and depressing levels of public sector debt is only one of several extremely concerning national economic statistics. A fresh-faced Labour Government is not going to suddenly bounce out millions of pounds any more than the current Conservative Government can. Academy Trusts must also be aware that there is the possibility that Labour's proposed plan to impose VAT on independent school fees would result in a sudden transfer of pupils into the state sector – with the financial impact unknown.

The list above is not by any means exhaustive when it comes to the issues facing the academy sector. Management teams and trustees will have to keep their wits about them over the course of the next nine to twelve months as monetary and political conditions increase the instability around the general economy and the academy sector.

Academies Accounts Direction 2023 to 2024 – What has changed?

By Magda Meier, Senior Manager (Education), Moore Kingston Smith

The updated Academies Accounts Direction was published on 27 March 2024 and will apply to accounting periods ending on 31 August 2024. Separate model accounts and an external auditors' guide were also issued, in a similar manner to previous years.

The updated guidance includes both explanatory and narrative changes. The requirements include some which will affect the contents of the narrative reporting and some which will impact the notes of the financial statements.

The following new requirements have been added:

- The **review of effectiveness of the system of internal control** (part of the governance statement) must now include a conclusion on whether the trust has an adequate and effective framework for governance, risk management and control. If the trust concludes that the system is inadequate, then the reasons should be explained and improvement plans outlined.
- Separate disclosure of material **non-GAG Department for Education (DfE)/Education and Skills Funding Agency (ESFA)** grants has been expanded to include 16-19 core education funding.
- The staff costs note has been expanded to include **Other employee benefits** as a separate line item. This will include non-monetary benefits such as medical care, housing or, cars.
- The **Agency arrangements note** has been expanded to include total cumulative unspent funds.

Other changes include the following:

- A new section **What an academy trust must do** has been added to the introduction page to provide a list of compliance related requirements.
- **Relationship with other financial returns** is also new and it includes two paragraphs explaining the relationship between the financial statements and the Academies Accounts Return (AAR). The section clarifies that the AAR is used to produce consolidated financial statements based on a different accounting framework (IFRS).
- References to the **Covid-19 supplementary bulletin** have been removed as the specific funding is no longer in place or has been incorporated into other funding such as Recovery Premium.
- Feedback to the sector from the ESFA has been updated to include the areas where **compliance could be improved**. Some of the areas highlighted cover late submission of the accounts, trustees' reports not reflecting current circumstances, and weak internal scrutiny arrangements.
- The guidance on the **Statement of Regularity, Propriety and Compliance** has been expanded to provide an additional example of sources of information reviewed by the Accounting Officer in forming their conclusions. The addition includes external assurance such as specialist reviews or inspections.
- The paragraph on the **Valuation of long leasehold premises** (from the Local Authority or other organisations) has been updated to include an assessment of the value of any assets from a transferring trust. It has also been clarified that DfE valuations, previously listed as a valuation source, are prepared under IFRS and assess value at the national, rather than local level.

The guidance can be found on the GOV.UK website and please get in touch if you would like to discuss in more detail.

Unlocking efficiency - Choosing the best financial software for academy trusts

By Danna Lukic, Director (Education), Moore Kingston Smith

Having the right financial software in place is key to the effective running of your trust. The right software can improve efficiency and accuracy if it can be integrated with other existing systems in place, or if it can produce the right outputs and reports needed by the trust, eliminating the need for manual data manipulation via spreadsheets.

Trust software being used should be reviewed on a regular basis to ensure it is fit for purpose. A review may be particularly beneficial if the trust has undergone or is planning significant growth or changes, such as joining or expanding a Multi-Academy Trust (MAT).

While there is some consistency in the academy sector, each individual trust is still unique and has different requirements and priorities. The trust's particular current and future needs should be determined, including but not limited to:

- the level and format of training and post-implementation support expected to be required;
- the level of integration with the trust's existing systems that may be required;
- whether the new system can easily produce management information that is important to the trust. In particular, does it facilitate the school-level and trust-level reporting that the various stakeholders expect?
- any other requirements of the system the trust would like to see, such as integrated fixed asset management.

Key providers

The Education and Skills Funding Agency (ESFA) has a helpful guide Choosing a trust's financial management system (FMS) (last updated in April 2024), which contains a table of academy trust accounting system software providers and helpful information available to aid initial comparisons.

It also details the spread of providers across the academy trust population based on information provided by the Academies Accounts Return (AAR.). This indicates that in the current year the market is dominated by the following key providers:

- IRIS (formerly PS Financials);
- Access/HCSS;
- ESS SIMS;
- Sage (including variations of Sage through their various business partners, who manage tailored Sage solutions for different types of academy trusts).

IRIS continues to have the largest segment of the overall market, particularly in the MAT market, being used by 30% of academy trusts, covering 45% of academy schools. Access/HCSS had the highest number of trusts submitting their AARs using automation. ESS SIMS focuses most on the SAT market of these key providers.

The guide is a useful starting point for trusts looking to assess the market, but trusts will clearly need to consider their specific circumstances before deciding which software providers to approach for more information.

What have we heard?

At Moore Kingston Smith we have found that many trusts are frustrated with working with outdated accounting systems; in particular, the following issues often arise, which have the potential to be solved by updated technology:

- connectivity issues for remote access;
- difficulty extracting data across multiple systems;
- poor reporting functionality requiring hours of manual labour, high costs and delays;
- difficulty accessing the right kind of training/support from the software provider;
- difficulties in adding new academies as a MAT grows.

We have seen a progression in the market with more options becoming available in the education space as the demand for systems which are cloud-based and user-focused grows. Accounting programmes like iplicit (which launched in 2023 and which has a MAT focus) have become more advanced and easier to use for the end-user, paving the way for more sophisticated reporting with quicker results.

Chart of accounts

A change in accounting software is an opportunity to consider transition to the DfE's Academies Chart of Accounts if you aren't already using it. This has been developed over a number of years, and maps directly to the Accounts Return and Budget Forecast Returns, enabling direct input of financial data into these returns.

Although the number of trusts using automation to submit their AARs is still small at 2%, there are a number of other benefits of adopting the Chart of Accounts, which is now being used by the majority of trusts (51%), including reduced subjectivity for mapping of nominal accounts and potential efficiency savings.

In summary

The trust accounting system is integral to operations, and should be fit for purpose for the trust's needs. It must be carefully chosen to align with the specific needs and requirements of the trust and offer a multitude of benefits, enhancing various aspects of financial management such as: accuracy, efficiency, cost savings, time management, enhanced communication and collaboration among team members.

Cyber vigilance - Enhancing security measures

By Richard Jackson, Strategic Business Manager, Moore ClearComm

Throughout 2023 the education sector continued to experience regular cyber attacks, with events reported weekly in the mainstream media. In addition, the sector started to see new and emerging threats arising from specific operational areas of their business model such as the Single Central Record (SCR), which gives cybercriminals extra leverage in ransom demands because of the atypically sensitive nature of data held by schools.

In this article we consider the current and future landscape, and in particular examine why Multi-Academy Trusts (MATs) incur increased risks, threats and recovery challenges post attack compared with schools operating outside of the MAT model.

A Global Challenge

Cyber attacks on schools, colleges or universities are not a problem unique to the UK. Forbes reported in March 2024 that, "...malicious actors' interest in the education sector is growing. Malware and phishing attacks remain the most prominent types of cyber

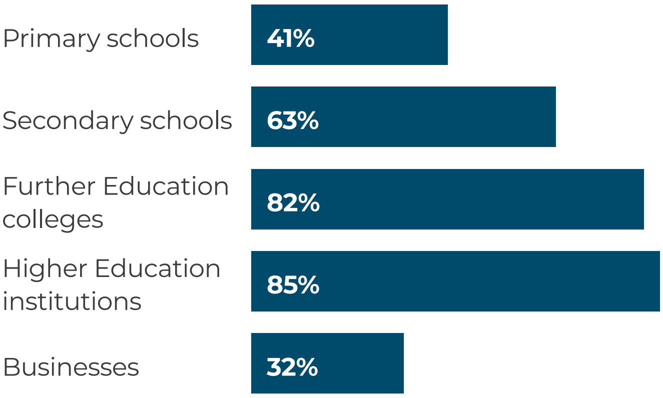
attacks in education, which ranks fifth globally by industry in cybercrime incidents."

The article went on to suggest that "cyber threats to schools and universities are escalating at an alarming rate."

Education in the UK

The latest National Cyber Security Centre (NCSC) research provides alarming evidence that the education sector is now considerably more likely to experience a cyber attack than the typical UK business. The NCSC reported that:

- all types of education institutions are more likely to identify breaches or attacks than the average UK business;
- education is now a more likely deliberate target for cyber criminals than commercial businesses;
- within the education sector, primary schools are the least likely to experience breaches or attacks – but even primary schools are more likely to be attacked than generic commercial organisations;
- further and higher education institutions are the most likely to be attacked.



The threat to MATs

MATs are a particularly attractive target for cybercriminals because centrally managed teams and systems for multiple schools innately create a wider threat surface for cybercriminals to attack via one attempt.

Through successfully attacking a MAT, cybercriminals can access vast amounts of data through a single attack, as opposed to attacking a single school site.

The more schools within a MAT, the more:

- attack surface that is constantly open to cybercriminal attention;
- likely it is that IT systems and technical security standards will vary from site to site;
- challenging and lengthy recovery can be from a cyber attack;
- likely attacks will be attempted (some schools/ MATs are attacked more than once each week).

Cybercriminals will research MATs extensively and assess key elements regarding which are the largest (and therefore may give access to higher returns) and which might have a lower than adequate security posture due to lack of awareness and investment (identifying which may be a soft target).

Looking at these numbers as an example, it is far more attractive to attack a MAT than to target a solo school (numbers are approximate at time of writing):

- 30 MATs include 26 schools or more;
- 85 have 12-25 schools;
- 250 have 6-11 schools.

It is no surprise, when looking at this data, that MATs represent a more likely target than single schools, though that is not to suggest that those single schools can assume their risk is low - quite the opposite is true.

What are cybercriminals trying to achieve?

All education providers retain a responsibility to be aware of the risk of fraud, theft and irregularity and address it by putting in place proportionate controls. This includes protecting against cybercrime.

Typically, any cyber attack will be carried out for one or more of six primary objectives:

1. Financial gain: the majority of attacks are designed to gain financially, with methods most often targeting employees via social engineering methods such as phishing or ransomware.
2. Insider threats: internal employees, vendors, contractors or partners can be approached by organised criminal gangs to attack from within, with this threat now seen as one of the greatest cyber security risks in 2024.
3. Political motivation: compelled by a specific cause, and likely to carry out an attack that renders systems inaccessible (Denial of Service).
4. State actors: criminals engaged in cybercrime to further their nation's own interests. Typically, they steal information, including intellectual property, personal information, and money to fund or further espionage and exploitation causes. Universities are particularly at risk, from an education sector perspective as these are often at the forefront of research in fields, particularly where foreign nation states may have specific interests in obtaining this intellectual property for their own economic benefit.
5. Recognition of achievement: cyber criminals are often competitive by nature - therefore these attacks are primarily driven by status and peer acknowledgment.
6. Corporate espionage: conducted for commercial or financial purposes, to gain an advantage over a competing organisation.

Considering the above, it is clear that the education sector should focus on protecting its key data such as:

- Financial systems
- Personal identifiable data
- Intellectual property
- Student coursework
- Staff personal records
- MIS/SIMS databases
- Single Central Record (SCR)

Successful cyber attacks will seize or render any/some/all of these areas inaccessible, which means that every school (and especially a MAT) will incur an immediate and potentially catastrophic challenge to overcome – with the clock ticking from the outset.

What can education providers do to minimise potential attacks?

Ensuring a strong defence against cyber attacks is more critical than ever. Every organisation must have measures in place to reduce the risk of fraud, theft and cyber incidents occurring; this risk is significantly heightened for MATs and the schools within each trust.

There are five key areas of focus for MATs to consider to mitigate the possibility of an attack:

1. Critical data: do you understand and manage the data assets held, and is access to this data adequately controlled?
2. Backups: are backups taken regularly, where are they stored, and is at least one backup not accessible from any system? Cybercriminals often target backups that may be accessible online as part of their attack to prevent a victim from restoring their data or systems.
3. Threats and vulnerabilities: do you understand the threats to your MAT and/or where you might be vulnerable?
4. Risk: is cyber security recognised as a fundamental risk to the operational resilience of the MAT, and therefore invested in appropriately?
5. Governance: are processes and systems in place to mitigate threats, and are they effective and tested?

Essential steps include (not exhaustive):

- Regular awareness sessions for staff and key stakeholders (including leadership teams and governors), in respect of threat awareness;
- Active network monitoring tools;
- Threat intelligence feeds;
- Zero Trust Security/Model;
- Cyber insurance;
- Security Information and Event Management tools (SIEM);
- Phishing simulation exercises (including physical/site access);
- Next Generation firewalls;
- Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS).

News in brief

Education sector insights

Independent advice on schools and teachers' pensions

The cyber threat to education and academy trusts in the uk

Top tips: what can you do now to prepare for a potential change of government?

How to get effective cost reduction right

What does the future hold for the world of payroll in the uk?

Tax facts 2024/25

2024 Events programme

Enterprise hub

Meet our education team

Anjali Kothari
Head of Education

akothari@mks.co.uk

Neil Finlayson
Head of Nonprofit

nfinlayson@mks.co.uk

James Saunders
Head of Academies

jsaunders@mks.co.uk

Luke Holt
Partner

lholt@mks.co.uk

Karen Wardell
Partner

kwardell@mks.co.uk

Jonathan Aikens
Partner

jaikens@mks.co.uk

James Cross
Partner

jcross@mks.co.uk

Dan Leaman
Partner

dleaman@mks.co.uk

Debbie Jennings
VAT Director

djennings@mks.co.uk

Ian Thomas
Director

ithomas@mks.co.uk

Tom Breading
Director

tbreading@mks.co.uk

Donal Moon
Employment Law Adviser

dmoon@mks.co.uk

Richard Jackson
Strategic Business Manager

rjackson@mks.co.uk

Dinah Patmore
Head of People Relations & Policy

dpatmore@mks.co.uk

CONTACT US

020 4582 1000
nonprofit@mks.co.uk

mooreks.co.uk

Moore Kingston Smith
**Top for
Overall Service
9 years in a row**
★★★★★★★★★
2023/24 Charity Finance
Audit Survey

MOORE Kingston Smith

Any assumptions, opinions and estimates expressed in the information contained in this content constitute the judgment of Moore Kingston Smith LLP and/or its associated businesses as of the date thereof and are subject to change without notice. This information does not constitute advice and professional advice should be taken before acting on any information herein. No liability for any direct, consequential, or other loss arising from reliance on the information is accepted by Moore Kingston Smith LLP, or any of its associated businesses.

Moore Kingston Smith LLP is regulated by the Institute of Chartered Accountants in England & Wales. Certain activities of the LLP and/or its associated businesses are authorised and regulated by the Financial Conduct Authority, the Financial Reporting Council or the Solicitors Regulation Authority. More details are available on our website at www.mooreks.co.uk © Moore Kingston Smith LLP 2024.