

AUDIT • TAX • ADVISORY

FE & HE Digest

Spring 2024

Latest news from the Further and
Higher Education sectors

Now, for tomorrow



An independent member of

bakertilly
INTERNATIONAL



Welcome to the Spring 2024 edition of our Further and Higher Education Digest.

We hope you all had a fantastic break over Christmas. 2024 is set to be an exciting year, and we hope the developments over the coming months will provide some more certainty for the sector.

Further Education Colleges are due to have sight of the Financial Handbook which will provide more clarity over the re-classification rules laid down by the Managing Public Money regulations. We are also expecting to have confirmation as to whether Further Education Colleges will need to change their accounting year end or not.

We are using this edition as an opportunity to reflect back on some of the lessons learnt from 2023 which include feedback from the ESFA on the new subcontracting standard. We also look at some common issues that arose during 2023 in relation to fraud and cyber security. Looking forward, we know that a number of colleges will be looking to enhance their ESG offering as well as looking to maximise their return on reserves, and so accordingly we have two articles that highlight where we can offer assistance.

As ever if there are any issues you would like to discuss further, please do contact any member of our FE/HE teams.

Best Wishes,
Further and Higher Education sector teams

Subcontracting Standard



Following consultation in 2020, the ESFA launched the sub-contracting standard and it was introduced from the funding year 2022 to 2023. The standard effectively acts as a license to subcontract. The standard is a requirement for any provider who subcontracts £100,000 or more of their delivery, across all ESFA funding streams. The standard sets out, in 10 sections, the requirements of the lead provider; in total there are 91 separate points.

Section	Points
Pre-award activities	13
Contract award and management	11
People	6
Administration	7
Managing relationships	9
Managing performance	10
Payments and incentives	5
Risk management	10
Contract development and/or termination	12
Provider development	8

The plan was that an external independent auditor would assess a provider's adherence to the standard and would then report back to the ESFA in the form of an assurance report. Upon receipt of the assurance report the ESFA would then review the report's findings, together with other relevant information, including locally held intelligence, to determine whether the provider has achieved the standard or not. More specifically, the auditor would report back whether the provider had:

- a) achieved the standard
- b) not achieved the standard, but would be able to do so if a series of identified actions, which would demonstrate compliance with the standard are completed. In this scenario the provider will be advised of the timeframe to demonstrate completion of the actions by the ESFA
- c) not achieved the standard and are required to cease subcontracting activities, until the ESFA is satisfied that the standard has been reached
- d) not achieved the standard and due to significant concerns identified either by the reporting auditors or by the ESFA results in a permanent cessation of subcontracting

The subcontracting reports were due to be provided to the ESFA by 31 July 2023 and it was hoped that the ESFA would be able to issue their responses to the reports 12 weeks later. However, this has been a huge challenge for the ESFA and in their December bulletin they issued an apology to say that there had been significant delays in the moderation process. The complexity of the standard and the varying audit report findings has made their task quite onerous. It is hoped that this might lead to a simplification of the standard going forward. We will update you in due course!

Advanced British Standard Consultation

Following the Prime Minister's announcement in October 2023 of the proposed launch of the Advanced British Standard, a consultation was launched on 14 December.

The consultation is seeking views on the design of the Advanced British Standard and is likely to invoke a number of views as the proposals are a significant change. We would encourage all Colleges to feed into this consultation.

Verification of Identity

Employers must verify the identity of the prospective employee by obtaining original, acceptable documents such as a passport, national ID card, or biometric residence permit.

Checking the Validity of Documents

Employers must ensure that the presented documents are genuine, unaltered, and belong to the individual in question.

Checking the expiry dates on documents is crucial to ensure ongoing eligibility to work.

Establishing the Right to Work

Different types of documents may be provided to establish the right to work, depending on the individual's immigration status. This could include a visa, residence permit, or proof of settled or pre-settled status under the EU Settlement Scheme.

Categorising Workers

Employers need to determine whether their employees have the right to work in the UK and categorise them accordingly, such as British citizens, European Union (EU) nationals, or non-EU nationals with valid work visas.

Recording and Retaining Documentation

Employers are required to make a clear copy or record of the documents provided by the employee.

This information should be retained throughout the individual's employment and for a specified period after their employment ends.

Re-Checking for Employees with Time-Limited Permissions

For employees with time-limited permissions to work in the UK, employers must conduct follow-up checks before the expiry of their current permission.

Keeping Up-to-Date with Immigration Rules

Employers should stay informed about changes in immigration rules and adjust their procedures accordingly to maintain compliance.

It's important for employers to follow these guidelines diligently to avoid legal consequences and ensure a workforce that is legally entitled to work in the UK. The specific details of the Right to Work checks may evolve over time, so it's advisable for your clients to regularly check for updates from the Home Office or seek legal advice to stay compliant with current regulations.

HR Solutions can support your clients with auditing how compliant their business is for Right to Work checks, completing Right to Work checks and advising them on Immigration matters for individuals requiring visas to work in the UK.



Changes to standing data

In 2023 the ESFA and Charity Commission both released guidance alerting Education Institutions to the ever increasing number of frauds that are occurring that involve fictitious changes to supplier or payroll details.

The fraud is widespread as it doesn't involve the fraudster gaining direct access to your systems. Instead the fraudsters use 'spoofing' emails to trick finance teams into making legitimate payments into the wrong account.

Here are two examples:

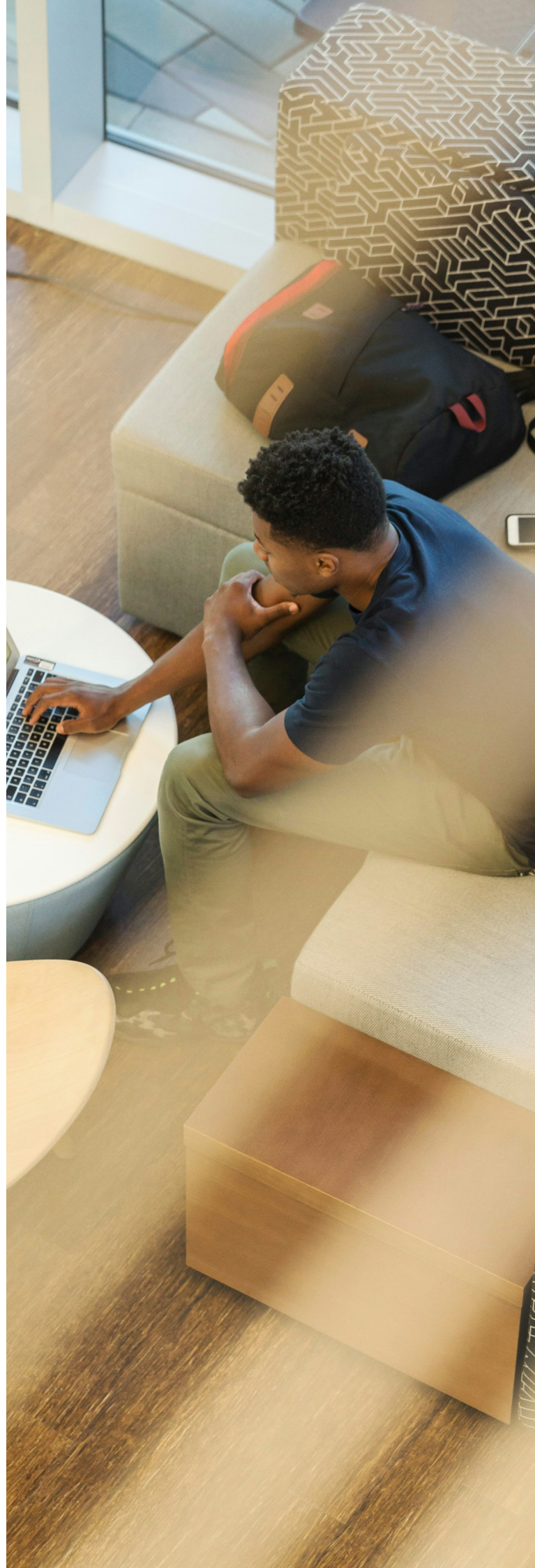
- 1** A day before running the monthly payroll an email comes in from the vice-principal saying that they changed banks earlier in the month but forgot to ask HR to update their details and so would the payroll team kindly take the email as instruction to pay their salary into the new bank account – details provided.
- 2** Early in 2023 the finance team are notified that a supplier's contact details are changing and they are given a new telephone number. Around six months later the finance team are expecting a large invoice from their contractor as they are part way through their transformational capital project. The invoice comes through as expected but the sort code and account number are different to the information they have on their system. A member of the finance team phones the supplier to confirm.

In both instances above, the emails came from fraudsters who masked the email address to make it look like it came from the legitimate source. If the fraud is successful it is very difficult to recover the funds.

The second scenario illustrates just how sophisticated these attacks have become with the fraudsters lying in wait for six months in order to perpetrate their fraud. With these attacks on the rise we have listed out a number of key processes that you may want to consider adopting:

- 1 The procedures for changing the standing data (bank account numbers, sort codes, contact details etc) of suppliers and staff should be documented in the financial procedures manual.
- 2 Never confirm the change of details by replying to the same address that the request came from.
- 3 Consider obtaining both written and verbal confirmation from suppliers to verify the change.
- 4 Aim to verify changes to details from other sources such as registered details on Companies House or company websites.
- 5 Changes to contact details should be viewed with the same scrutiny as changes to banking details.
- 6 Where possible make use of self-service portals – for example, changes to payroll details can only be accessed through a HR portal which can only be accessed using the College's secure network
- 7 A log of changes to standing data should be maintained. This log should detail what procedures were undertaken and by whom in order to verify the change.

Most importantly, we would urge all educational institutions to be very vigilant in this area. We advocate discussions amongst the finance team to both highlight awareness but also to ensure procedures are known and are adequate.





ESG In Education

Many educational institutions have already begun their Environmental, Social and Governance journey. At MHA we have supported a number of clients by using our own expertise and experience from our own journey. One of the keys to success is requiring a commitment from the top but also support from stakeholders at every level.

Educational leaders, governors and boards recognise that their core constituents – students, faculty and staff – want to be part of a purpose-led organisation. A deliberate, robust and intuitive ESG strategy, accompanied by a coherent action framework and transparent communication, will help educational establishments attract students and their parents/guardians, attract staff and enhance relationships with community, supply chain and governing organisations.

Because ESG is all about continuous improvement it sits naturally within the educational environment and addresses many core educational issues. ESG embraces ethics, service, protection, benefit, integrity and responsibility and a commitment to sustainability is particularly important to students and faculty.

The success of your ESG actions rely on a collaborative and collegiate programme involving governors and leaders, staff, faculty, students and your supply chain.

Key questions include:

- 1 What internal forces are encouraging your ESG focus?
- 2 What are your core constituents?
- 3 What commitments are they seeking?
- 4 Which environmental issues and risks are most material to your establishment?
- 5 How far are you prepared to commit?
- 6 What are your feasible goals?
- 7 Will your strategy include operational changes?
- 8 Will you effect behavioural change?
- 9 What are your current and planned energy sources?
- 10 What is your energy budget?
- 11 Which sources of clean energy are available to you/appropriate?
- 12 What infrastructure changes are feasible?
- 13 Which actions will have the highest impact?

We are expecting to see a continued emphasis on ESG from various stakeholders and funders. We have seen how corporate codes of governance have now codified these considerations into the governance processes within organisations. So if you would like to hear more about the services we can offer please do get in touch.



Environmental

Energy use, renewable energy sources

Waste management

Attitudes and actions towards climate change issues

Supplier management

Investment policies

SECR – consideration is advised even when not in scope



Social

Working environment and culture

Student learning environment

Employee and student health and safety

Compensation practices

Diversity, inclusion, policies to prevent sexual harassment

Training and professional development



Governance

Diversity of governing board, academic councils and other standing bodies

Financial accounting and transparency

Executive compensation

Ofsted compliance



Cyber Security arrangements – common weaknesses and how to address them

MHA's Internal Audit teams have carried out a number of Cyber Security and IT Health-check reviews across the previous 12 months in response to the elevated level of external (and potentially internal) threats within this area. Whilst the outcomes of these audits have differed from organisation to organisation, as you might expect, a number of common areas of weakness have been noted, the most frequently observed being in respect of activity directory management (access controls over IT systems and directories). We have therefore set out below some of the common failings observed, together with highlighting some of the controls that should be established over this area to reduce the risk of system compromise in the event of a cyber-attack.

Common Weaknesses

The following control weaknesses have been observed across our audits in respect of the general management of system and user access to IT systems:

- Outdated policies and procedures which do not reflect National Cyber Security (NCS) Guidance
- Leaver accounts still active after the employees had left, in some cases for more than one year.
- Accounts established with a 'cannot change password' setting enabled, meaning users cannot change passwords themselves, even when they may be concerned their password has been compromised.
- Accounts established with a 'password never expires' setting, which may mean that older passwords which do not comply with current password practices might still be in use and these are more likely to be compromised in the event of a cyber-attack.
- Service accounts (accounts which have some form of service functionality) having passwords which have not been changed for over 10 years.
- Password length and complexity below what is recommended within NCS guidance. Such guidance recommends the introduction of minimum password lengths of 10 characters, or three random words approach, and further guidance can be found [here](#).
- No process of review between the IT user database and HR database to ensure only active employees have their accounts enabled on the system.

In addition, for elevated privilege groups the following was observed:

- Default administrator accounts still named as such and not changed to an anonymous name. This could make these accounts more vulnerable to cyber-attacks.
- High numbers of staff having access to privileged accounts where such access may no longer be required. This presents would be attackers with more accounts to try to hack which have enhanced levels of access.
- Multi Factor Authentication (MFA) not in place for gaining access to privileged accounts.

What controls should be established to reduce the level of risk in this area?

NCS Guidance recommends a number of controls and processes which should be established in respect of this area, and further guidance can be found [here](#). The key actions in respect of this area are summarised below.

Develop and embed appropriate policies and procedures. Such procedures should set out:

Who should have access to which system and / or data and why. This should include consideration of part time staff, volunteers and contractors in addition to full time employees.

- The policy should detail what and how audit records are acquired, how they are safeguarded against tampering and what authorisations are required to access them.
- In addition, the policy should include a section on account management for new starters, movers and leavers, whether full time or otherwise.
- The arrangements in place for how third parties who require access to your systems can do so and what authorisations and disclose agreements are required.
- Finally, the policies should outline what your organisational entities work email address are able to be utilised for e.g. what websites and services staff can access using their work email account.

Implementing multi-factor authentication for all user accounts where appropriate. In doing this it is important to consider:

- That the type of MFA utilised is proportionate to the level of risk faced. For example, any accounts for online services should have MFA implemented to protect against password guessing. If there is the potential to do so, offer users the choice of how to authenticate (e.g., SMS, email, software etc) so that the approach can operate across different users and locations.

- Where passwords are required, implement a password policy that balances usability and security.
- Ensure credentials are adequately protected both at rest and in transit.

Implement MFA and other controls in respect of privileged accounts with increased access levels, including:


- Consideration of the level of privileges that should be allocated for such accounts, and only providing full privileges where it is absolutely necessary for domain admin or cloud admin accounts.
- Ensure that MFA is enabled for these accounts and consider the use of strong authentication methods for these, using risk based decision making depending on the levels of risk associated with the accounts and the nature and volume of activity.
- System administrators should have separate user accounts for their day-to-day business (e.g. email access) and for their administrative activities. These two accounts should be separate from each other, including use of separate devices with any unnecessary web or email access blocked from the admin account to limit the level of exposure to phishing attacks.
- There may also be some benefit in considering the above approach for accounts for users who are able to authorise high value financial transactions or make changes to key software systems.
- A regular review should be carried out regarding who has been provided with privileges and these should be removed when they are no longer required.

Finally, it is important that appropriate security monitoring tools are in place to detect potential malicious behaviour.

This should include:

- That there are systems in place for logging and monitoring authentication and authorisation events so that suspicious behaviour that may indicate a potential compromise can be detected.
- Such a monitoring system should be designed so that any activity performed and system used can be identified against the person who performed and used them.

.....

 If you require any further information in respect of the above, or would like further assurance over your key IT systems and controls in place, then please do not hesitate to contact chris.rising@mha.co.uk for how we may be able to assist further.

Wealth Cash Service

With rising interest rates making cash-based deposits more attractive in recent years, savers and investors are looking for ways to make their money work harder.

We understand that for most further and higher education institutions, cash management doesn't justify a huge investment of time or resources. It's easy to default to your existing bank but the interest rates may not be competitive. It's also likely funds are not fully protected on the Financial Services Compensation Scheme (FSCS). This is precisely where our preferred cash platform can help.

The platform helps treasury and finance teams manage cash with minimal effort by unlocking hundreds of cash deposit products from investment grade banks, across multiple tenors and currencies.

The cash platform is designed to complement the day-to-day bank account by offering the following features:

- **Support** – A dedicated relationship management team working directly with your treasury and finance functions from the initial call, through on-boarding and portfolio management.
- **Bank Panel** – Diversify your cash deposits with more than 30 banks (investment grade and challenger) and building societies on the Insignis Bank Panel offering a variety of term options to meet your liquidity requirements. This includes easy-access, notice and fixed term accounts.

- **FSCS protection** – Available for the first £85,000 per banking institution. By holding cash across different bank providers, it's possible to secure 100% FSCS protection.
- **Personalised Illustrations** – Bespoke illustrations providing access to attractive rates, some of which are only available through our cash platform provider.
- **Security** – Dual authorisation available on all transactions.
- **Reporting** – Access seamless reporting and execution of all deposits across all banks and building societies in one place.
- **Beneficial Ownership** – Your business remains the beneficial owner of the funds at all times.
- **Simple Application** – One application form at the outset means the cash platform can be accessed as soon as the account is open, providing access to over 30 banks. No other forms will be needed in the future.

As at 12th January 2024, competitive interest rates for corporates include 4.65% for easy-access, 5.15% on a 3-month fixed term and 5.15% for a one-year fixed term.

The cash service can be accessed for sums over £250,000 and a more comprehensive 'hands on' service is available for sums over £5m. The experienced cash team will work with you to navigate this process and deliver a solution that works.



Please contact the MHA Caves Wealth Team to arrange a non-obligatory discussion.

Meet our Further & Higher Education sector experts



Rakesh Shaunak
Managing Partner
& Group Chairman



Rachel Doyle
Partner



Sudhir Singh
Partner
Head of Not for Profit



Stuart McKay
Partner



Chris Rising
Internal Audit Director



Andrew Matthews
Partner



Mark Eagle
Audit & Outsource Director



Rajeev Shaunak
Partner



Nicola Mason
Director

MHA Caves Wealth is authorised and regulated by the Financial Conduct Authority (FCA), Financial Services Register number 143715.

Risk Warning

This is a marketing communication for general information only, and is not intended to be individual investment advice, a recommendation, tax, or legal advice. The views expressed in this article are those of MHA Caves Wealth or its staff and should not be considered as advice or a recommendation to buy, sell or hold a particular investment or product. In particular, the information provided will not address your personal circumstances, objectives, and attitude towards risk. Therefore, you are recommended to seek professional regulated advice before taking any action. We are not providing advice or a personal recommendation in respect of the cash service offered. The rates illustrated are a guide only and should not be relied upon. The interest rates are subject to change. You may decide that based on the financial strength of these counterparties, or on the appeal of individual products, to allocate funds to just one or two institutions. The level of diversification, whether from a counterparty risk or liquidity risk perspective, is entirely at your discretion.

mha.co.uk

 @MHAaccountants

 MHA

Now, for tomorrow

An independent member of
bakertilly
INTERNATIONAL