Frank Field
Education Trust

Future Multi Academy Trust (MAT) consolidation is inevitable but how will this happen?

By Dr. Chris Hampshire MBA (Dist.) PhD

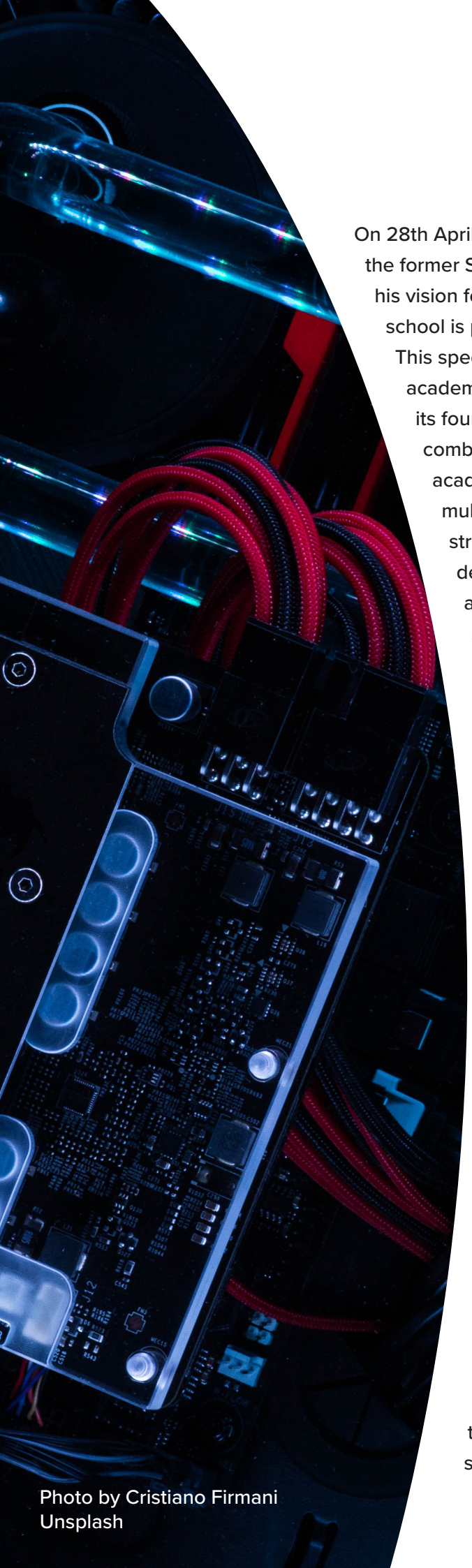


Photo by Cristiano Firmani
Unsplash

Frank Field
Education Trust

On 28th April, in his speech to the Confederation of School Trusts (CST), the former Secretary of State for Education, Gavin Williamson, outlined his vision for the future of the state-funded school system, where every school is part of a 'family of schools in a strong multi-academy Trust'. This speech, went beyond simply supporting the current multi-academy Trust system, built on strong multi-academy Trusts as its foundation, by suggesting an end to the current pick-and-mix combination of LA maintained, empty MATS and standalone academy schools. The rationale behind this endorsement of the multi-academy Trust education system was a belief that the strongest leaders can support more Trusts and schools whilst developing staff, thereby allowing schools to focus on teaching and learning - ultimately leading to improved outcomes for students.

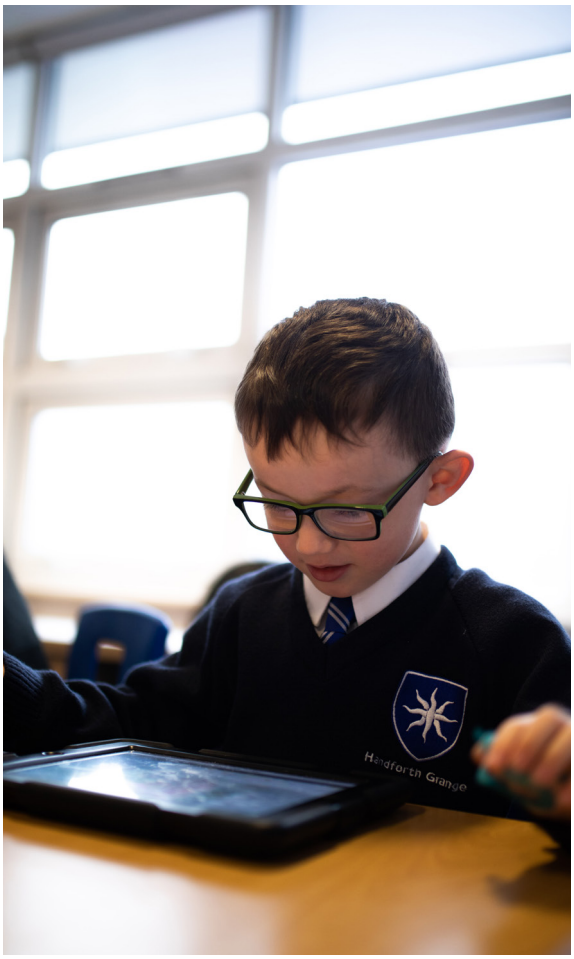
The thread through the speech was the impact of strong governance, across groups of schools, which has the potential to deliver a greater impact than other models. This point was reinforced with the confirmation that the Government does not consider single-entity Trusts to be a viable proposition. As a result, the future is likely to see the growth of multi-academy Trusts through mergers of Trusts and/or conversion of schools into the existing multi-academy Trusts.

For academy Trusts looking to expand, this provides a clear indication that the Government is committed to a fully academised state-school system that includes consolidation of multi-academy Trusts across England. In some circumstances, maintained schools will be directed to join a particular MAT and will have little, if any, input into that decision. Underperforming LA schools, judged by Ofsted to be inadequate, will be issued with an academy order by their Regional Schools Commissioner (RSC), requiring them to become an academy and join a MAT specified by their RSC.

This paper is not aimed at schools looking to choose a MAT to join as, it is aimed at MATs who are looking to grow through the integration of other Trusts, or welcoming maintained schools.

In 2020 alone, the ICO fined various organisations for differing GDPR breaches including:

- Ticketmaster UK Limited fined £1.25million for failing to keep its customers' personal data secure as it failed to put appropriate security measures in place to prevent a cyber-attack on a chat-bot installed on its online payment page.
- Marriott International Inc fined £18.4million as it failed to put appropriate technical or organisational measures in place to protect the personal data being processed on its systems.
- British Airways fined £20m for processing a significant amount of personal data with weaknesses in its security measures when solutions were available at the time that would have prevented the successful cyber-attack.
- Cathay Pacific Airways Limited fined £500,000 for failing to protect the security of its customers' personal data as the IT systems were accessed via a server connected to the internet resulting in malware being installed that harvested data. A catalogue of other errors were also found including: back-up files that were not password protected; unpatched internet-facing servers; use of operating systems that were no longer supported by the supplier and inadequate anti-virus protection.
- DSG Retail Limited fined £500,000 after a 'point of sale' computer system was compromised as a result of a cyber-attack due to vulnerabilities such as inadequate software patching, absence of a local firewall, lack of network segregation and no routine security testing.



All MATs incur costs in establishing and maintaining IT systems, IT infrastructure and IT security and the ICO indicates that the costs of maintaining appropriate IT security measures can be used when deciding what security steps a MAT needs to take. However, the ICO states that steps taken by the MAT must be appropriate both to the circumstances and the risks that the IT systems and the IT infrastructure creates. In order to address this, a MAT needs to develop and implement security steps that ensure the confidentiality, integrity and availability of the IT systems and services and the personal data processed within them. In addition, a MAT needs to take steps to enable IT systems access to be restored in a timely manner should a physical or technical incident arise. These steps should be supported by having appropriate processes in place that test and validate the effectiveness of the measures deployed, including a regular detailed IT risk assessment.
As can be clearly identified from the above, there is a significant financial risk to a MAT of an ICO fine following an IT data breach which is likely to be regarded by the ICO as non-compliance with GDPR. It is therefore imperative that a MAT identifies all the IT risks and puts in place mitigating actions to address each risk as the ICO will take into account both the technical and organisational measures applied by the MAT when considering if any fine should be incurred and if so, how much.

GDPR security principles cover a MAT's processing of personal data; not just cybersecurity and includes confidentiality, integrity and availability of data.

Frank Field Education Trust

So what administrative and IT security measures does a MAT need to consider to address all obligations to comply with the legal and regulatory aspects of GDPR?

In simple terms, the administrative and IT security measures a MAT puts in place need to ensure that the data is:

- Only accessed by those authorised to do so; within the delegated authority limits.
- Accurate and appropriate to why the MAT is processing it.
- Accessible and usable. Therefore if any personal data is accidentally lost, altered or destroyed, the MAT must be able to recover it in a timely manner.

Whilst GDPR does not actually define the security measures that a MAT should have in place, the GDPR principles do require a MAT to have a level of security that is appropriate to the risks presented by the processing of the data within the MAT. GDPR takes a risk-based approach to information security which means that different solutions will be used within each MAT as these solutions will be dependent upon each MATs circumstances and the associated risks that these potential solutions can address.

All IT cyber-security measures deployed must be appropriate to the nature of the personal data held and should include the following:

- System security and cyber-security measures appropriate to the size and use of the MAT's IT network and Information Systems.
- IT data security covering all the data within the various IT application systems and appropriate to the business practices operated by the MAT.
- Online security that includes covering the security of a MAT's website as well as all other online services and application systems used.
- Device security including policies on Bring-your-own-Device (BYOD).
- Current IT developments including the cost of deployment and ongoing maintenance of any counter measures deployed.

The government's Cyber Essentials scheme includes a base set of security controls that a MAT can put in place relatively easily https://www.ncsc.gov.uk/cyberessentials/overview. However, Cyber Essentials doesn't address the circumstances of each MAT or the risks posed by every IT processing operation. Therefore, it is likely that a MAT may need to go beyond these base set of security requirements, depending on the actual processing activities undertaken on the personal data.

There are a number of approaches that a MAT can take to better understand the IT risks including developing and establishing a MAT IT Strategy which covers:

- Assessing current IT setup

  This should include an IT Technical Audit with a RAG report in plain- English, broken down by the areas of technology across the MAT but also for each school within the MAT. This should produce an external benchmark into the health of your current IT set up that will identify options on what to do next.

  Having this initial RAG report of the current IT estate within the MAT is however just one half of the knowledge a MAT needs. A wider review is needed that includes the MAT employees who use the different IT systems regularly for teaching and non-teaching and back office administration.

- The next stage is to identify and agree the Target Operating Model (TOM) based upon the detailed understanding of where the MAT is now, both in terms of the current IT estate and the MAT employee usage and would include an indication of what options are available, at what cost and by when.

- Agreement of the TOM then results in a detailed plan being produced that identifies how the MAT moves from current IT set up to the agreed TOM.

- The final phase is executing and delivering against the plan which may well include phased implementation of the different solutions being deployed. Each phased implementation should then result in an assessment of the effectiveness of that solution.

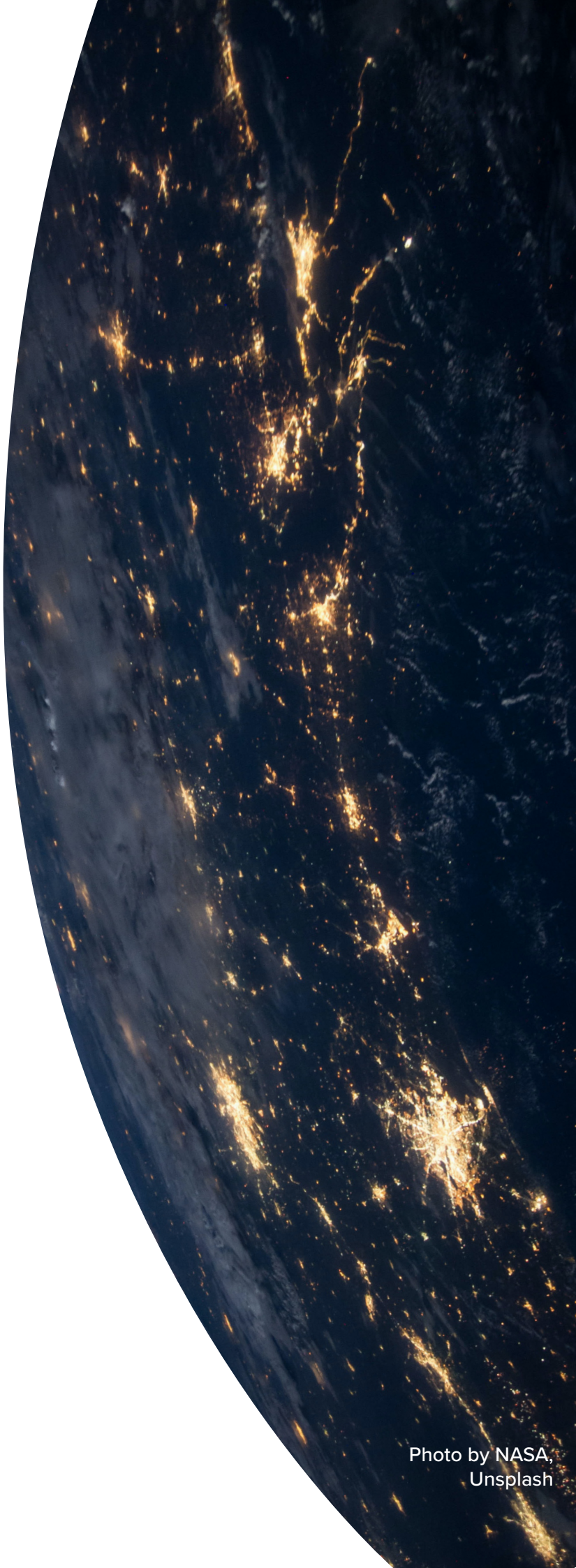


Photo by NASA, Unsplash

Frank Field
Education Trust