COVER STORY

Getting ready for GDPR

The General Data Protection Regulation will take effect on **25th May 2018**

Establish a squad of **data privacy 'champions'** in different areas of the school

A **full audit and assessment** of practices should precede any attempt to update the privacy policy

Pro-active steps to GDPR compliance

Hopefully, whether or not you read the introductory piece in the Summer 2017 edition of the Bursar's Review, the concept of the General Data Protection Regulation (GDPR) should not be new to you – and its impact day of 25th May 2018 should come as no surprise.

For those of you who may have heard tell of the new UK Data Protection Bill, this does not change matters – it was an expected step to bring GDPR into UK law, regardless of Brexit. It was also necessary to fill in a few gaps which the EU left to individual governments to take a particular view on.

Those familiar with the existing Data Protection Act may recognise some of the language in the UK Bill around exemptions for areas such as safeguarding and employment. By next year we may be referring to 'DPA 2018' rather than GDPR – but do not for one minute think that the GDPR compliance standards you have heard so much about in the past year will not still be a part of our law.

Core themes of GDPR

When advising schools on the impact of GDPR, I have been keen to emphasise three things:

1. Data protection is not simply an IT issue; it is a cultural one. It hinges most critically on the human factor, both in respect of the individuals ('data subjects') that the new legislation places at the heart of the law, and the organisations that are, themselves, primarily made up of people.

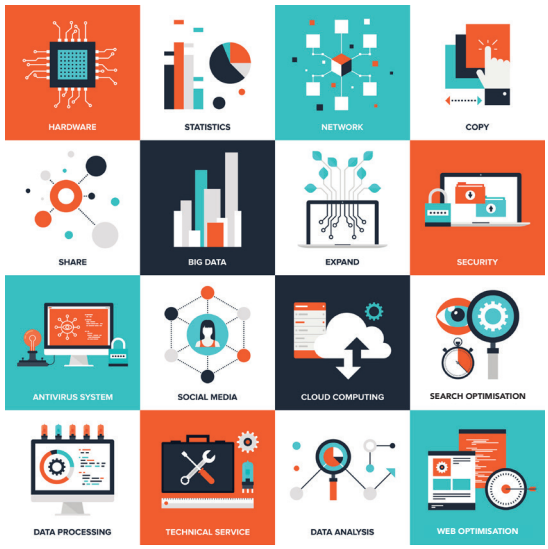
2. Good communication is vital to obtain the buy-in necessary to embed GDPR in your organisation – again, this means your communication to staff as well as to the pupils and parents (past, present or prospective) that will make up your 'data subjects'.

3. Policy is part of culture and communication. It should exist as a living thing, not a piece of paper kept in a drawer or posted on the website and forgotten about. What is more, good policy should not simply be downloaded wholesale off a website.

I will deal with the last point first, but return to it at the end (you must trust me that there is method in the approach!).

How to update your privacy policy

Many schools will share much of the same DNA, perhaps, in terms of what should go into the core privacy policy – but in order to get there it is critical to conduct a sweep of systems and data at your school. This is not simply an exercise in box-ticking or a way for lawyers or GDPR consultants to earn money. Not only is it critical to gain, and keep, this degree of corporate knowledge in-house – it is also something that, in terms of record-keeping, the regulator will expect to see has been conducted. The quality of your systems review prior to GDPR will be a major enforcement and compliance factor should the school's data protection practices be questioned by an individual, or in the media (for example due to a privacy breach or fundraising 'scandal').



The phrase used to describe this process is called many things by different people – a data asset sweep, a DP audit, a systems review – but ultimately it fits within a term of art within the GDPR called a 'privacy impact assessment' (PIA). There is no set form to this, because a PIA can be short or long, and may concern new projects or a risk assessment of how things are done already – but the most major one a school is likely to undertake is the one that should be underway already.

We will return, then, to the privacy policy later; the key message here is *don't put the cart before the horse*. In other words, you cannot expect to give an accurate description to the world at large about how you process personal data until you have a good grip on it yourself.

Where IT systems and culture combine

As above, I emphasise that GDPR is not an 'IT problem' – this is primarily to give a wake-up call to those (and there are many!) who have tried to pass the buck to the technical department, claiming all this 'data stuff' is not their area. In fact, compliance is an issue that starts with the foot-soldiers – any of whom could make a mistake for which the school could be legally liable – and goes all the way up to the board of governors, who are expected to have full visibility of (and take responsibility for) the issue of data privacy at the school.

However, this is not to play down the importance of IT. In a modern school it has a big role to play; if data protection law may be characterised (very broadly) as the way the law describes human interactions between organisations and individuals, then as we know, an increasing majority of those interactions now happen (and are recorded) digitally. This goes particularly for email, intranet, e-filing and record-keeping – as well as automated systems, monitoring and storage.

Alongside systems that are secure and fit for purpose, what is equally important is how humans and IT combine. There are two sides to this coin:

1. How do staff record information? How do they use email? Are they aware that, with only limited exceptions under subject access rules, anything they say about an individual (colleague, pupil or parent) could be provided to that person on request? Are they aware of the need to be accurate, and not excessive, in how they 'record' information about people – given how long the memory of digital data is?

2. How prepared is your school to deal with requests from people? For the reasons set out below, your ability to deal effectively, promptly and proportionately to these requests will in large partly depend on the quality of your systems.

Dealing with data subjects

Under GDPR it will not simply be subject access (which itself is a huge burden, and the response time is being reduced from 40 days to 30). Additional subject rights will include:

1. The right to object to certain ways in which you process their data – not just an automatic right to object to marketing (including fundraising), but also to challenge where you are relying on 'legitimate interests' to process their data. This is even more critical because of the ease with which individuals can now withdraw any consent previously given. Schools may still have valid legal grounds to process, but the burden will be on them to show it – or the ICO could make them stop. *This emphasises the need to have systems and records in place such that these questions can be quickly and confidently answered, and those answers supported by policies and PIAs.*

2. The right of rectification or erasure of data (sometimes called 'the right to be forgotten'). This right is by no means absolute, but again you will need to be there with prompt and ready answers; why do we need this data? How did we get it? Does the purpose still stand? And for justified complaints; how easy will it be to fix? *This emphasises the need for systems which are readily accessible, searchable and amendable – as well as containing key data points like, what category of data is this, how did we get it and, what legal grounds are we relying on to use it?*

3. The right of 'data portability' – if someone transfers to a different school, for example, they have the right to ask that all their personal data records are copied across to the new school.

This emphasises the need for systems to keep personal data in organised, intelligible and transferrable formats.

Bursars will need no reminding of how hard subject access requests can be to deal with; these new rights further up the stakes. But the positive spin is this; think how much easier your life would be already if your systems were this efficient!

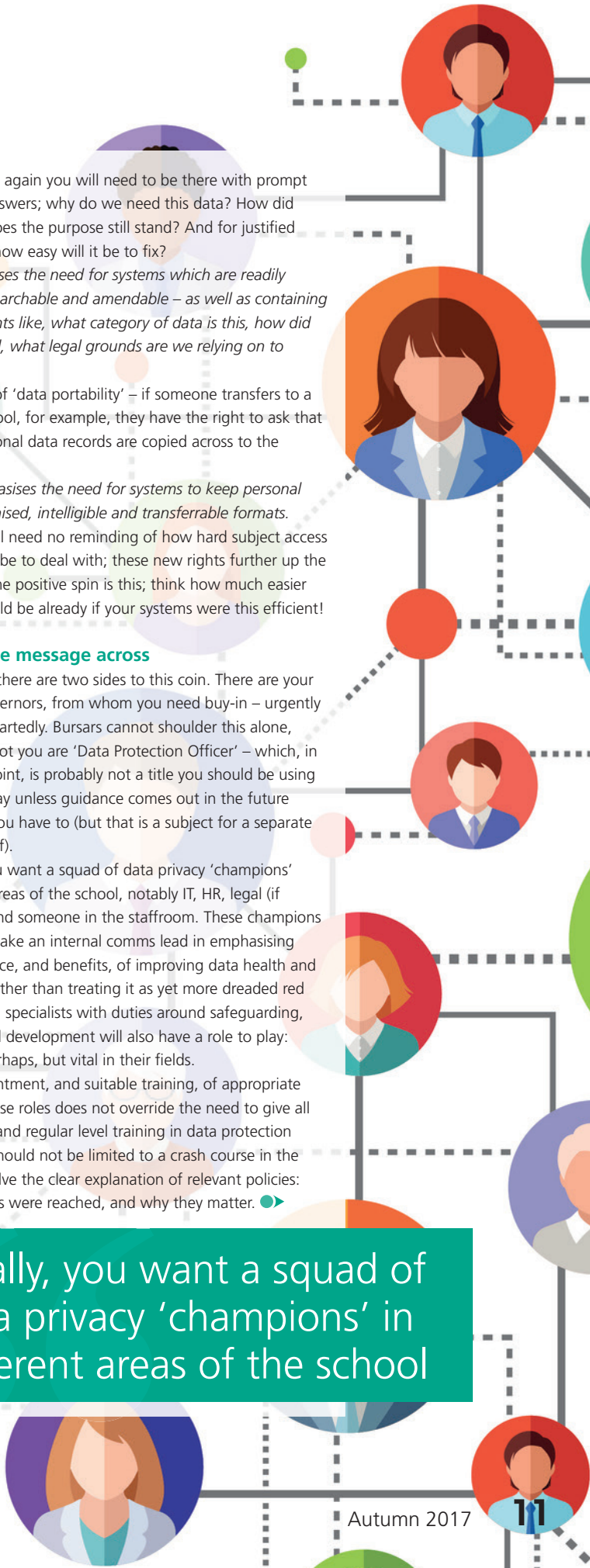
Getting the message across

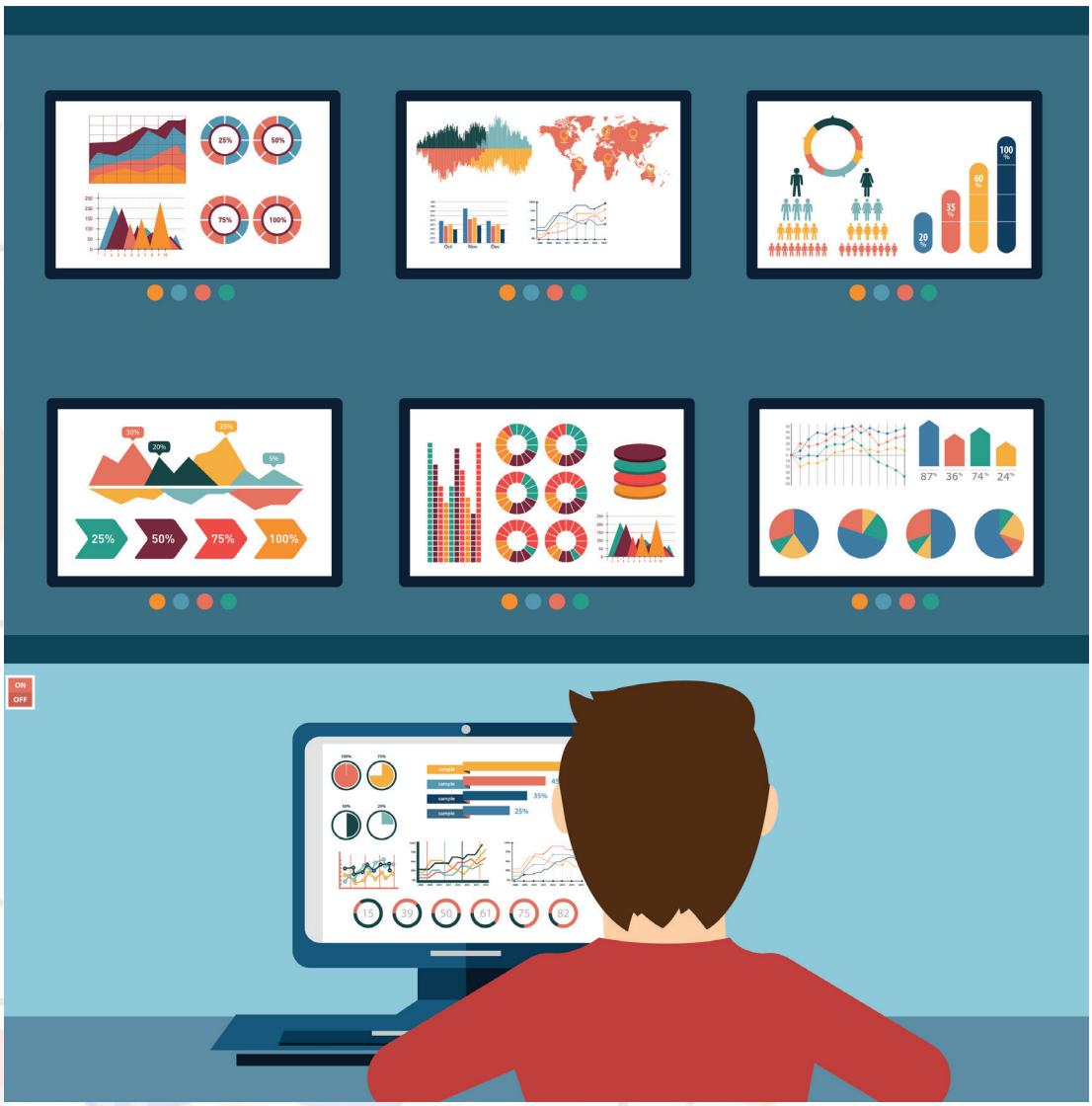
Once again, there are two sides to this coin. There are your staff and governors, from whom you need buy-in – urgently and wholeheartedly. Bursars cannot shoulder this alone, whether or not you are 'Data Protection Officer' – which, in a separate point, is probably not a title you should be using from next May unless guidance comes out in the future saying that you have to (but that is a subject for a separate article in itself).

Ideally, you want a squad of data privacy 'champions' in different areas of the school, notably IT, HR, legal (if applicable) and someone in the staffroom. These champions will need to take an internal comms lead in emphasising the importance, and benefits, of improving data health and practices – rather than treating it as yet more dreaded red tape. Existing specialists with duties around safeguarding, archiving and development will also have a role to play: narrower, perhaps, but vital in their fields.

The appointment, and suitable training, of appropriate people in these roles does not override the need to give all staff a basic and regular level training in data protection issues. This should not be limited to a crash course in the law, but involve the clear explanation of relevant policies: why decisions were reached, and why they matter.

Ideally, you want a squad of data privacy 'champions' in different areas of the school





Wearing another hat, staff are also the school's data subjects and so will need to understand and have provided to them relevant policies that affect them directly; CCTV and acceptable use of IT, for example. If the school is using safeguarding monitoring software or introduces a policy of recording all low-level concerns raised about staff, then this needs to be clearly communicated.

All of which leads us back round to the question of updating policies. This is critical again to ensure buy-in from parents and pupils, so they understand how data is used; the parent contract will play a role, along with permission and contact forms (when they start and leave the school), and so will your new privacy policy. Hopefully, the message is clear that the full audit and assessment of practices should precede any attempt to update the privacy policy – and when it is ready, it should be rolled out and actively provided and explained to all those it affects.

The ISBA, with Farrer & Co's advice and input, will be providing guidance and resources for all its members in the coming months along these very lines. However, the message, in the meantime, is that schools need to be taking their pro-active steps to 'own' compliance, to update and prepare systems as necessary, and to get a comprehensive picture of what personal data they already hold, process and intend to keep going forward.

Author
Owen O'Rorke
associate at Farrer & Co

020 3375 7348

GDPR case study

Toks Oladuti, director of information systems at the Francis Holland Schools Trust, says that the Trust's journey to achieve General Data Protection Regulation (GDPR) compliance began in the spring term of 2016, with a review of how it was meeting the requirements of the UK Data Protection Act (DPA).

With the EU's GDPR on its way in, I decided to launch a Trust-wide programme to be compliant with GDPR well in advance of May 2018. I also wanted to ensure that we would end up with a streamlined and easy-to-manage core policy, and have procedures in place to embed good data protection practices into all our activities.

As the Trust's data protection officer (DPO), the first port of call was to start raising overall staff awareness on data protection and the incoming regulatory changes. This was achieved through briefing sessions and workshops, with particular focus on promoting good data protection as a positive thing and something we should all be striving to deliver. We also focused on data subject rights and definitions of key terminology such as 'processing', 'controller' and 'processors', and the types of personal data. It was fundamental that staff understood the wide scope that the term 'processing' covered, such as storing, analysing and sharing data.

Once awareness levels had been raised, it was imperative to gain a complete and thorough understanding of all the personal data that we processed in the Trust and how we processed it. Gaining this knowledge was achieved through a series of compulsory staff questionnaires, workshops and electronic discovery searches on digital storage locations. The questionnaire was followed up by meetings with departments dealing with a large variety of personal data or special categories of data, such as learning support, admissions and the bursary.

Risk management

From this, I was able to produce a register of every processing activity and method, including the legal basis for collection, usage, storage and sharing. This register was then reviewed with the rest of the senior leadership team, guided by the Regulation, to quantify the risk and compliance levels of each activity with its principles (i.e. lawful, fair, transparent, for a specified purpose, etc).

With the register detailing the risk level and procedures of each processing activity, it was simple to apply risk management. For each activity, a decision was made to accept the current risk, reduce the risk through GAP analysis and implementing change, or avoid the risk by dropping an activity. Each one of the risk management decisions was documented in the register to form the foundations of our internal record keeping, a key requirement in being able to prove compliance. Whilst some activities were easy to assess, there were some that presented a challenge.

Challenges

Some of the areas where we spent a lot of time were to do with teacher mark books and planners, bursary data, alumni relations, fundraising, physical (paper) data and data within emails.

With teacher mark books and planners, we had to take into consideration their various formats (paper, electronic and cloud-based) and the differing types of content. It was important to fully understand how critical these were to staff in their planning, day-to-day teaching and classroom management, but still weigh this against the need to fulfil our data protection responsibilities. Our approach was to specify that staff can use mark books and planners to store academic data, but that pastoral, learning support and sensitive data had to be coded. Additionally, regular backups of the data had to be saved onto the central storage platforms. We decided that electronic mark books and planners needed to be reviewed and authorised to ensure compliance, particularly with rules surrounding processing data outside the EU.

The bursary processes significant data about pupils, parents and staff, with some of it being very confidential or of a special category. A review found that this data was already being processed centrally and in a compliant manner. Additionally, it was important to work closely with the bursar to update our retention schedule for the variety of data processed, based on their operational needs and multiple legislative requirements regarding finances, employment and health and safety.

We were in a good position with alumni relationships as we already required consent to sign up. With fundraising, it quickly became apparent that whilst compliant with the DPA, our consent forms and notification would need updating and renewal for GDPR.

Updating the data protection policy

Another issue was tackling the multiple copies of data that were in use. It was not atypical for the same data, such as a file, to have physical copies (in filing, folders and on notice boards) and electronic copies (in personal drives, shared drives and emails). It was important to get the balance right between reducing this duplication and maintaining its usability. We ended up changing relevant processing activities to focus on centralising a large amount of data electronically, as single copies in the core management information systems (MIS) or network drives.

Armed with a final register of processing activities, the next phase was to update our data protection policy and conduct a review of all internal policies and supplier contracts. The data protection policy update was guided by our processing register and included key procedure guidelines, including those covering the updated data subject rights. We included the requirement for a data protection impact assessment (DPIA) to be completed during the development of any potential school activity that will include data processing. This will support the ethos of data protection by design and default, and contribute to our internal record keeping. The overall policy review was primarily to check other policies for cross references to data processing activities and to ensure they remained compliant.

Suppliers' responsibilities

Given that some of our suppliers are data processors, they have enhanced responsibilities under GDPR. It was therefore necessary to perform a compliance review on existing contracts and contact those where an update was necessary. Some suppliers already had updated terms and others have promised that these will be completed before the May deadline.

On track!

We are on track to be fully compliant for GDPR this year, with a few final tasks left to complete. Refreshed data protection training is being integrated into all staff inductions, and a programme of training sessions and workshops is scheduled for this academic year. Our amended data protection policy is going through final ratification and updated privacy notifications are awaiting final approval to go live later this year.

From conversations that I have had with other schools, I think that whilst there is a lot of good guidance out there, most would like information that is more tailored to schools and a bit more directional. My advice to schools would be to talk about GDPR to each other and within groups such as the ISBA. I still feel that awareness levels and actual activity regarding GDPR needs to increase across the education sector. As a minimum, I would suggest doing the following:

- Designate someone to assume the responsibilities of a DPO[1] who has seniority and will have authority over the data processing activities. Provide them with training where necessary and seek professional advice. As an International Association of Privacy Professionals (IAPP) member, I have had training and have continual access to a wealth of other privacy practitioners and lawyers for advice and queries, which has been invaluable.
- Promote an overall sense that data protection is not a constraint, but a positive opportunity to handle personal data in a secure and fair manner.
- Deliver briefings or workshops to all staff, so that they are aware of the incoming regulation and understand the key terminology, such as processing and what actually constitutes personal data.
- Find out all the personal data that they process and how – this can easily be achieved through compulsory questionnaires for all staff (full and part-time), followed up by meetings where necessary for clarifications.
- Perform and document a risk assessment on your processing activities.
- For high risk processing or those without lawful basis, agree on a plan of action to address it.
- Decide on what information you will allow in mark books and planners.
- Decide on acceptable information that can be emailed.
- Centralise as much data as possible – use your MIS or well-structured and secured shared drives.
- Update your data protection policy.
- Update your privacy notices.
- Review contracts and terms with suppliers who are data processors (i.e. online MIS, online payment platforms, etc).
- Where consent was previously obtained by opt-out methods, re-obtain consent.
- Train staff on the new or updated policy and ensure that data protection becomes an integral part of all school operations.
- Maintain awareness throughout the year through briefings, INSET sessions or workshops.
- You need to be able to prove compliance, so document and maintain records (even a basic spreadsheet or register) of all processing activity and data protection decisions.

There is time, but not much, so dedicate the personnel and other resources needed to complete your journey to GDPR in time for 25th May 2018.

[1] It is the view of Farrer & Co that schools will not have to appoint a DPO and, indeed, to give the appointee that title could bring unnecessary and burdensome regulation on the role. The ICO may yet offer guidance that schools fall into the categories of those who need formal DPOs, but until they do schools may wish to use an alternative title like 'Head of Data Compliance'.

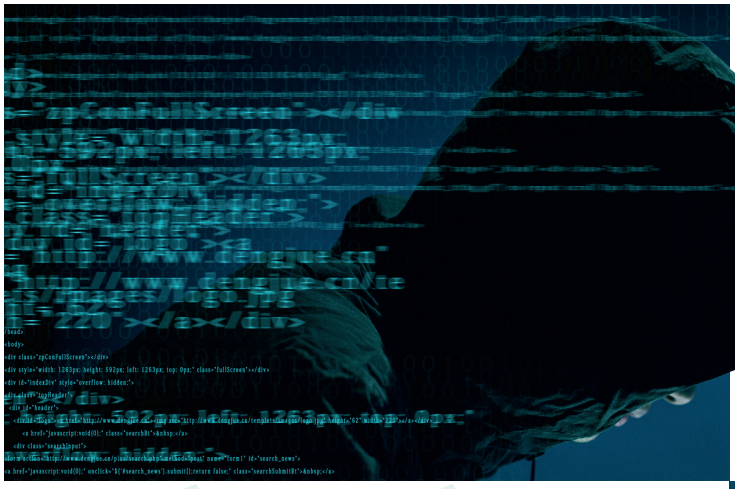
Know your weaknesses

- **All** websites are vulnerable
- **Assess vulnerabilities** after every update of CMS software
- Assess the risk to **all** your web facing platforms

The practical obligations of GDPR

With GDPR fast approaching, *Mark Orchison*, managing director of 9ine Consulting, explains how schools can avoid common cyber security pitfalls.

At the heart of the GDPR is strong governance. In the event of a data breach, organisations will need to demonstrate to their supervisory authority (in the UK this is the ICO) the mechanisms they have in place to manage compliance with the regulation. This incorporates the initial process to become compliant and then the ongoing maintenance of those structures so that at board level, organisations have the confidence that their governance structures are effective.



Additionally, the GDPR mandates third party assessment of those governance structures. A critical part of compliance is having the confidence that your ICT systems, operating policies and processes are sufficiently robust given the types of data processing activities, and that cyber security vulnerabilities are known and managed. Article 32 of the GDPR requires schools to evaluate the technical and operational risks, taking proportionate mitigating actions given the evaluated risk.

Within a cyber security context, school leaders need to understand the primary areas of concern, the risks these pose to the processing of data and an appropriate mechanism to determine what proportionate mitigating risks would be.

The following are recent examples of common cyber security vulnerabilities within schools which can be easily identified and mitigated against:

Website security: school websites and web-facing school systems are easy and available platforms for a cyber security breach. In a recent case using a widely used website content management system (CMS) two critical vulnerabilities were identified within the school's CMS which could have allowed a hacker to become a 'man in the middle' to gain admin credentials. This then would have provided access to the management console of the website, and consequently, have the potential to compromise other systems that are visible via the website.

> School leaders must be provided with weekly and monthly dashboards on key factors affecting operational management of technology

Other vulnerabilities in other website content management platforms can allow a potential hacker to substitute the logon pages a user would use with the hacker's own code and logon script. By doing this, the hacker has compromised the system and has all the credentials of users of those systems.

The important lesson here is that all websites are vulnerable and require regular assessment for vulnerabilities. A proportionate response may be to assess vulnerabilities after every update of the CMS software or, as a minimum, annually.

Web application security: Similar to the school website there will be other systems that school users regularly access via a website or web portal. These systems can be hosted by the school, however, in many cases these are hosted by the application provider. Examples include learning management systems (LMS), virtual learning environments (VLE), alumni, safeguarding and management information system (MIS) platforms. These systems are open to risk from the same risks posed to websites and additionally, through risks from users with access to these systems. In the example of a VLE, it is quite possible that a student could compromise the system and gain access to all other user data on the VLE. Or, credentials are compromised through the website example and then used to gain access to other systems that, in turn, are further compromised.

A proportionate response with these systems could be to assess the risk to all your web facing platforms, taking into consideration the types of data shared/stored and conduct annual or version release web application penetration testing.

Web-facing systems: every school is likely to have servers that are the school gateway to the internet. These systems are published to the internet via their IP address. Examples include, locally hosted email, locally hosted VLEs, locally hosted CMS systems and filtering platforms. Vulnerabilities in regard to these systems relate to the firmware, operating systems or public information that these systems publish (depending on their configuration). It is not uncommon to find vulnerabilities in these areas, which then can allow a hacker to take control of the schools core systems.

A proportionate response may be to assess the public facing IPs and school systems, conduct a vulnerability assessment (that is relatively straightforward) and then a more in-depth external systems penetration test.

Internal penetration tests: When conducting internal tests, all a potential hacker needs is physical access to the school. This could be access to a network port or, even easier, access to connect to the school wireless system; which can be achieved by sitting in the school car park or road outside the school. In a recent example of a large independent school with a complex and robust architecture; a professional test hacker was able to obtain domain administrative access within two hours, achieving this with little knowledge of the school network and the use of basic hacking techniques that someone with only an interest in hacking could replicate. Risks such as these can be mitigated through having full system documentation, regular vulnerability assessment and annual internal penetration testing. The downside of this mitigating action is that the cost of putting things right can be very high. The cost is commonly disportionate to the immediate organisational or performance benefits gained; however the mitigating actions are more often than not, proportionate to the rights and freedoms to the data subject (as determined by the GDPR) given the types of data processing activities within a school.

Approved code of conduct

Within the regulation and specifically Article 32-1a and Article 32-3, it is a mandatory requirement for organisations to understand the effectiveness of their IT systems and also to adhere to an approved code of conduct. With the latter, this means successful completion of the cyber essentials certification and with the former; the organisation must be able to provide hard data to demonstrate that the operational management of their IT systems is effective. In practice, this means that school leaders must be provided with weekly and monthly dashboards on key factors affecting operational management of technology.

All in all, the GDPR places significant practical obligations on schools, and importantly, obligates schools to seek appropriate and proportionate professional support given the risks to the rights and freedoms of data subjects whose data they control.

Author
Mark Orchison
managing director of 9ine Consulting, technology, cybersecurity and data protection specialists

www.9ine.uk.com