GDPR:
THE COUNTDOWN CONTINUES

Published by Sec Ed and Headteacher Update

The new General Data Protection Regulation comes into effect in just under three months' time. Al Kingsley advises...

On May 25, the General Data Protection Regulation (GDPR) comes into effect, which leaves schools little time to get prepared.

Until very recently, local authorities had not provided enough clear information to schools on how they should be tackling the issue. Thus, schools have been left to decipher what is fact vs fiction and what are the right and wrong ways to handle the requirements from the mixed messages they receive.

There are many voices on GDPR, from those warning schools about the risks to those which are simply scaremongering.

The background

When we talk about legislation in education, it tends to be that the local authority or academy trust disseminates any important updates to its schools on any changes that need to be made.

However, with GDPR, it hasn't been this way. The difference is that GDPR isn't just for schools – it applies to every organisation that handles the personal data of individuals, be that students, customers, employees, passengers, patients, prisoners (the list goes on).

As such, the Information Commissioner's Office (the UK authority on GDPR) has issued generic, all-encompassing guidance that organisations must read and interpret before deciding how it applies to them and the way they operate. This means there is no specific guidance for schools – there is no specific guidance for anybody. And that's why a degree of scaremongering and panic has ensued.

Preparation is key

With the implementation deadline of May 25 fast approaching, the key challenge for schools is to find out what they need to do and to do it now. The starting point is the 12 steps set out by the ICO (see further information). Essentially, this is the blueprint to compliancy, so if your school can get these areas covered, then you are home and dry.

The good news is that schools are used to keeping records and adhering to procedures, so much of what you are already doing will apply to GDPR – you will just need to check that you are doing it in line with the requirements. For me, the key areas schools need to take into account are as follows.

Training

The senior leadership team will need to extinguish any prevailing negativity about GDPR and how "complicated" it is and get their staff on board. By doing so, staff will begin to see that it is for everyone's benefit. They must primarily be aware of the 72-hour deadline for reporting any data breach and the need to follow any new procedures the school puts in place to ensure the security of personal data. Perhaps consider appointing a number of staff GDPR champions as a rotating responsibility to answer the questions of others. This way, everyone will eventually become familiar with the requirements.

Data discovery

To be able to protect data pertaining to individuals, you need to know where it is located. This applies to paper and online files and documents – including where there may be duplicate copies or where staff are retaining their own versions. This is often a time-consuming task, but schools can be helped by software solutions that seek out every GDPR data-type file on the network.

Data protection

It is important for schools to know that the software and apps your school is using are GDPR-compliant – i.e. the data these applications collect is not excessive and that it is kept sufficiently secure. You will need to keep a record in line with this requirement and again, there are software solutions that can help with this.

Data breaches

As mentioned, all data breaches must be reported within 72 hours and all

staff must know this. Again, everything must be recorded as evidence of what happened and whether the data was at risk. For example, if a teacher left an unsecured USB stick in a classroom PC overnight, the school should be able to prove via its records whether the data was encrypted, whether the PC was accessed and whether the classroom was locked.

To help prevent data breaches, schools will also need to ensure security measures are in place on their network, e.g. adequate antivirus protection, security alerts to notify technicians of multiple login attempts from a particular machine and so on.

Individuals' rights

When a request is submitted to the school to disclose or delete an individual's data, you will need a workable procedure in place to deal with this. So formulating a detailed process for how your data is collected, used, stored and shared is essential.

Use "what if?" scenarios to help you. For example: what if a parent wanted all data held about their child disclosed to them? Which member of staff would be responsible for finding it, collating it and sending it to that parent? Who would record that process, and how?

Data Protection Officer (DPO)

Schools must appoint a DPO and this must be an appropriate person who is impartial and does not have a conflict of interest.

The ICO has issued general guidance about the DPO role (see further information) and is of the view that there is no reason why a DPO cannot know the staff or pupils in the school – i.e. why the DPO cannot be a member of school staff. However, according to the ICO, what would prevent a member of staff taking on the DPO are:

- If they didn't have enough experience or knowledge of data protection law, bearing in mind the complexity of data processing in the school, and the level of protection required.
- If they didn't understand how data in the school was used.
- If their professional duties aren't compatible with the duties of the DPO and lead to a conflict of interests.

In my view, there is simply too much grey area when it comes to what schools can and cannot do in the proper implementation of GDPR and this is one example. Yes, school staff can be DPOs provided they "have enough experience/knowledge of data protection law" – but with pressure on staff (especially teachers) coming from all sides, expecting them to find time to delve into data protection law on top of everything else could well prove be the straw to break the camel's back. Ultimately, it's better clarification and more transparent guidance that schools need right now. How are schools supposed to evaluate what constitutes a "conflict of interest"? How can individuals know if their professional duties are not compatible with that of a DPO? This is where the existing guidance falls short.

I for one would like to see more specific guidance on how the DPO role can work in schools, especially in terms of what constitutes a conflict of interest. In the meantime, I know that some schools are finding that reciprocal arrangements with other schools or a suitably qualified governor or trustee could be possible solutions to the DPO issue.

Evidence

Record and report everything. This evidence is your safeguard should the worst happen and a data breach occur in your school that requires investigation.

Next steps

It is important to remember that GDPR isn't something you need to get ready by May and then forget about. Therefore it is better to empower and enable schools to be self-sufficient, rather than have to pay someone continuously to come in and do the work. However detailed GDPR is, it is really not rocket science and with some time dedicated to it now, there's no reason why a school shouldn't have measures in place in time for the deadline.