# WHAT DON'T WE KNOW ABOUT GDPR?


Published by Primary School Managment

Over the last couple of months, the Information Commissioner's Office and the DfE have gone almost overboard in sharing lots of information about what the incoming general data protection regulation means for schools. However, a few grey areas remain.

In terms of where schools are likely to fall short of meeting their GDPR obligations, data retention is likely to be top of the list. Schools are good at policy-based reporting, and having overarching governance ensures that people follow policy, but keeping their data stored in a secure location, and making sure that data gets deleted when it's supposed to be, will be more of a challenge.

It's unclear what the penalties for GDPR non-compliance might be at this point. Schools will likely encounter issues if they have a data breach, or if a former employee requests data that the school's unable to provide, but in general I think there's been a fair amount of scaremongering around GDPR. I don't believe it's credible to claim that schools are going to get charged millions for GDPR failings.

The ICO (ico.org.uk) is obviously a good starting point for obtaining further information about GDPR, and The Key (thekeysupport.com) has some great resources for leaders and governors. The National Governance Association (nga.org.uk) produces some useful checklists to help governors scrutinise what's happening in their schools and ensure they ask the right questions.

Depending on your school's status, your LA should be able to provide GDPR-related guidance and training. There may also be teaching schools offering GDPR courses in your local area, and further information can be obtained from national events, such as the upcoming Academies Show (academiesshow.london).

There's a wealth of resources out there, but at the same time, many schools have been left to interpret vague GDPR guidelines for themselves and decide how best to implement them. This has resulted in confusion and even compelled some to enlist paid-for consultants, who are only too happy to offer their services. Here, then, are several areas where GDPR guidance remains unknown or unclear, and what schools can do to address them:

## Data Protection Officers

One thing that's presented a challenge for lots of schools has been appointing a data protection officer (DPO). It's a key role, which involves ensuring that a school is meeting its GDPR reporting obligations, where the DPO needs to be one step removed from the data to avoid a conflict of interest.

The ICO has stated that DPOs can be teachers, but I'd suggest that's not entirely appropriate. There can't be that separation of interest with a business manager in the role, since they're responsible for staff payroll and other bits and pieces, resulting in uncertainty as to whether schools should appoint a governor, a trustee or a paid data protection officer of some kind.

The advice I've given to the schools we're involved with is that appointing a governor or trustee would be appropriate, as long as they're suitably trained. Not so long ago, financial management standards in schools (FMSiS) stated that governors could serve as responsible officers with oversight of a school's financial practice. I'd say the same could apply with DPOs.

## Obtaining Consent

Most data processing in schools comes under the umbrella of 'public interest'; they can have it because staff need it to perform their jobs, but certain areas likely require consent. Schools will be used to having to obtain consent for educational visits or photography, but the obligations are now much broader when a school stores, for example, parental information and contact details. There are now whole areas where schools need to seek consent again per item – 'global consent' will no longer be possible.

## Subject Access Requests

If an ex-member of staff asks for details of everything you've stored on file about them, do you know what that entails and the timescales involved? Many schools haven't yet thought through the procedures they'll need for subject access requests. Which form gets filled in? Who handles it? Who coordinates enquiries and locates the relevant information?

The typical turnaround time for these will be a month, rather than the previous 40 days. If I submit a request as an ex-member of staff, the SBM's got to look at my personnel file, teacher records, performance management, appraisal data and more. The volume of files and data potentially involved could be quite significant.

## Data Breaches

A data breach could involve something as simple as a memory stick left in a PC overnight, or a PC being left unattended with some personal information about a child displayed on screen. As well educating staff about the small things they might not consider to be data breaches, schools need to think about how breaches are handled and recorded. Small incidents, such as notes left on desks and emails sent by accident, won't necessarily need to be reported to the ICO, but schools will need to record and log them.

## Data Discovery

Many schools don't quite appreciate how far-reaching the GDPR's data discovery requirements are. This refers to all the information schools hold not just digitally, but also physically. That cupboard full of old files from years ago that nobody dares open? Its contents relate to the records you hold.

In terms of digital data, we're talking all files stored locally on PCs, as well as email archives and any details you might still have of people who applied for a job a year ago (the latter of which shouldn't still be on file). I don't think it's been spelled out to schools yet just how far reaching the information they hold actually is, and what the process of discovering where it's all stored will entail.