GDPR:

1) "A practical guide for understanding and implementing GDPR". (Separate document see link on OGA website)

   This document was written by a law firm which specialises in providing GDPR compliance for its Corporate clients. It has not (yet) been amended to meet the specialist needs of schools, and does not pretend to do so.

   However, it does explain the technical terms and the key measures contained in the GDPR legislation, so that you can get to grips with both the high-level objectives of the legislation, and also its technical detail.

   It also contains advice on whether or not to appoint a DPO, and what the role of the DPO is.

   It also discusses in-house staff training, which will affect many more members of staff than is often assumed. All teaching staff including TAs, HR, Finance, SLT all will need some training. This doesn't have to be extensive, but it needs to be flexed to meet the needs of individual departments. "One size" will not "fit all".

   What it *doesn't* go into in sufficient detail is the fact that there are much tighter regulations around "medical" data. This element of the legislation is principally aimed at companies such as Health Insurance or who work in the Health field exclusively, who ONLY deal with medical customers. It is my personal opinion that this will be a particular concern for schools, who have a small but constant proportion of pupils whose primary presence in school is education, but whose needs are also medical. This will obviously have the greatest impact on special schools but it will also affect all schools. 2 GDPR specialist firms have been asked questions about this, and neither has known the answer! It seems it hasn't been thought through by anyone (I stand ready to be corrected on this.)

   Important: this document is for information purposes *only*, and should not be relied on / used as a substitute for professional (paid-for) advice. It is designed to inform governors so they are sufficiently expert to provide their normal levels of challenge to HTs / SLTs.

   Please also note that the NGA is strongly advising AGAINST individual governors becoming the GDPR specialist / even DPO for their school(s).

2) First thoughts on how the advice in the booklet could be flexed to meet the needs of schools.

   This section has been written by a member of the OGA with some expertise in the area. However, it does not aim to provide anything other than help in how to *think about* implementing GDPR within your school. **Again, it must not be relied upon as formal advice.**

First Thoughts Section

Training and Accreditation.

Accreditation is thin on the ground. However, there is a US body called the IAAP who offer a DPO qualification, which is being introduced into Europe. To gain IAAP accreditation, you have to sit a series of taxing exams – it's no "degree-by-post". However, at this time, many people who are offering GDPR advice will not be IAAP accredited. My personal advice would be to favour a supplier offering

IAAP accreditation, but not to treat it as essential. (Again, this is a personal view, and not a formal recommendation).

Webinar

https://www.esentire.com/gdpr/

There is a great deal of information out there. I would recommend the above webinar as being the most useful. It is about "Moving up to GDPR" – so presumes some knowledge of existing Data Protection Law. However, a modicum of knowledge / common sense should suffice.

You have to register to watch it. Simply put in your school / academy email address, and say your job title is Compliance Officer, or CFO / Head of Finance etc., and you should receive an email giving you permission to watch it.

I had to listen to it 2 or 3 times, taking frantic notes, before I got the best out of it, but I thought it was time well spent.

Information Commissioner's Office (The ICO)

With regard to the ICO, all the thinking has been about medium to large commercial concerns. The ICO has recognised that there are specific challenges for small companies, small statutory bodies such as Parish Councils, and Charities and has provided specific guidance for them. They don't mention schools. And it seems pretty clear that schools haven't got on the ICO's radar as yet.

However, there *are* lots of useful templates on the ICO website which could be adapted for schools - the text is well written and clear and repays at least a browse.

The information I received from the Webinar identified above, is that the ICO want to build up a body of case law in this field, to define their role more closely. To do this, the current thinking is that they won't be going after the really big boys, because they don't have the staff to chase down huge multi-nationals. They are equally not interested in corner shops etc. They will start by going after the mid-sized companies. This would seem to preclude schools, at least in the early months / years.

However this is only someone's personal opinion, and should not be used to delay working on GDPR compliance. Proving you've made a good start is the bare minimum; I would suggest (personal opinion only).

Your first steps in achieving this is to write:

1) A public **Privacy Notice** for your school website.
This is the annoying thing you now get when you log into any website / phone any call centre. It is relatively easy to do – there is specific wording on the ICO website, and you just need to bang it up.

2) **Data retention policy**
You urgently need to think through, and write, a Data Retention Policy. To an extent, GDPR is a bureaucratic exercise about policies / procedures etc. – schools are so used to doing this, we may actually be at an advantage compared with many businesses.

The key question is, how long should schools retain data once pupils and staff have left the school. In a commercial environment it's clear you must delete data once your "relationship" has ended, but with former pupils, when does that relationship end? There seems to be no clear answer as yet – (again I stand ready to be corrected). A Data Retention Policy will be of help, here.

A Data Retention Policy lists which data classes / types you retain, and outlines how long you decide to keep that data, together with an explanation of your decision making process, and which of the 6 criteria your data class falls under (consent, contract, public task, legitimate interest...see guide for list and explanation). i.e. examples you might include in your policy would be to:

- Retain all pupil data pertaining to results for 5 (?) years after a pupil leaves so that we can write references for future employers / future schools. This could be justified under Public Task as Education is statutory. Consent if we've obtained it, or Legitimate Interest criterion. It doesn't matter which criterion you choose, as long as you can justify and document your decision making process.
- Retain pupil data relating to children with an EHCP for 10 (?) years to ensure appropriate continuity of care for vulnerable children. This could come under heading of Public Task or even Vital Interest as at risk children can indeed be in danger of their lives. We would also have to append details of additional data security measures we will put in place to meet the higher demands of retaining medical data.
- Retain staff employment data for 5 (?) years after a teacher leaves the school to allow us to meet our responsibilities under the Safer Recruitment requirements.

These are just 3 examples – there will be many more. You need to think it through for your own school. I don't know if other schools / authorities have yet written a Data Retention Policy which we can cannibalise?

Does a diagnosis of ASD / ADHD / dyslexia etc. constitute a medical record?
It seems very likely that pupils with ASD, ADHD, dyslexia diagnosis etc. would qualify as a medical record, and enhanced data security measures will be necessary. Many pupils with ASD etc. are identified as SEN, but don't require an EHCP, so these would have to be a special class within your Data Retention Policy.

The terms are also bandied around quite liberally by members of staff - if a record is kept against a pupil's name in a class register, for example, that could possibly cause problems.

Finally some thoughts on finding appropriate professional help.

Companies offering GDPR services tend to come from 2 different skillsets:

1) IT system security / management / integrators background - who tend to treat the whole thing as an IT issue. IT plays an important part in GDPR compliance, but it is NOT, at heart an IT problem, it's a Privacy problem. Suppliers from an IT background may not understand the cultural needs of a school.

   This doesn't mean that an IT solutions provider is a bad choice, but I would suggest you interrogate them carefully about their process, before appointing. If it's just about IT, you might only be getting half the picture.

2) Legal / compliance background - who might be more skilled at seeing outside the constraints of IT. However, their focus tends to be on acting in such a way to protect their clients from legal entanglements, which may be too "lawyerly" for you needs. It's about interviewing carefully, and finding out if they understand / can meet the specialist needs of schools.
   Academies and MATs have external legal providers – if your existing law firm has a GDPR offering, it may be worth investigating this as an additional service. You already know they are an education specialist. However, if they're not correctly geared up to provide GDPR services, they are the wrong suppliers – GDPR skills outweigh educational knowledge, I would think.