COVER STORY

Getting ready for GDPR

- The General Data Protection Regulation will take effect on ***25th May 2018***
- The regulator, expects you to ***hit the ground running***
- ***ISBA*** will publish ongoing GDPR guidance on its website

NEW DATA PROTECTION REGULATION:
one year to go. What you should be doing now

Owen O'Rorke, associate at legal firm Farrer & Co, talks us through the practical steps schools can adopt to prepare for GDPR.

The General Data Protection Regulation (GDPR) will take effect across the EU, including the UK, on 25th May 2018 – in less than a year's time.

For some bursars, this change will have been right at the top of their agenda; others, perhaps understandably, will have put this to one side until one *absolutely* has to make changes. Unfortunately, this moment has certainly arrived.

There is no further grace period for adjustment once 'DP-Day' hits during the next academic year: we are already half way through the two years allowed for transition, which began on 25th May 2016, when the final text of the new law (which will replace the Data Protection Act 1998) was published. Once it applies, schools must be ready and compliant: the Information Commissioner's Office (ICO), the regulator, expects you to hit the ground running.

Compliance challenges

This quick summary of action points is aimed at those who have perhaps been slow out of the blocks in preparing for the GDPR. Whilst there is no shortage of professional advice about GDPR out there, it is worth bearing in mind that the basic structure and principles of data protection law will remain the same. If you have managed to instil good habits ●➤

▶ The new regulatory environment brings new compliance challenges

and introduce effective policies in your school to date, you will be well on the way to compliance.

However, there is no doubt that the new regulatory environment brings new compliance challenges, and an increased need for transparency and evidence-based accountability, on top of the already clear trend of stricter enforcement by the ICO. To date, independent schools may have avoided the harshest forms of ICO penalty but – as many will have noted with concern – charitable status is no longer (if it ever was) a basis for 'special consideration' in compliance standards, nor a shield to public criticism and fines. The 13 fines issued to charities by the ICO in the past six months for using personal data unfairly, specifically in a fundraising context, ought to have brought that point home.

Checklist

The issue of compliant fundraising and alumni practices weighs heavily on development offices, with many considering a move to 'opt-in only' consents (both going forward and in respect of historic databases). Others are considering legitimate interests as a legal basis for continuing to process personal data and communicate with alumni in the future, although this approach has limitations – certainly where electronic means of communication are concerned. The ICO is reluctant to accept that more intrusive activities such as wealth screening can be justified without consent.

This question goes beyond GDPR, and requires more space for discussion than we have here. Given the inherent risks and also its commercial importance, it is ideally a topic for specific advice, both legal and practical, for each school according to their needs, ethos and risk profile. This article is aimed at explaining the wider impact of GDPR and the steps required for readiness more generally.

ISBA and the Institute of Development Professionals in Education (IDPE) will be publishing new GDPR-facing materials and policies in the months to come, beginning with the template 'data protection audit grid' referred to below. Please log in to the ISBA website for more information about how this will be disseminated in coming months and, for the time being, familiarise yourself with the checklist below.

- **Identify a compliance lead within your organisation, and raise awareness.** This may, of course, be you. Even if your school does not legally require a formal appointment of a data protection officer by law, under the GDPR from May next year, you will need someone within your school to take responsibility – whatever their job title. This does not have to be a stand-alone, full-time role, and you may require assistance from those with IT or HR roles – but it is important not to silo this as a 'technology issue'. Data protection compliance is a top-down issue, senior management within a school should be involved in driving this forward, and it goes far beyond your IT set-up.

- **Ensure you are on top of the ICO guidance.** There is some GDPR material already available on its website **https://ico.org.uk/** although less than expected at this stage. The diversion of Brexit was perhaps to blame for this backlog, but since government confirmation that the GDPR will take effect as planned, a busier programme of new ICO guidance is now expected in 2017. New consent guidance (following consultation) is due shortly, and there is also relatively recent guidance on Privacy Notices (i.e. your Data Protection Policy).

- **Carry out a mini-audit of the personal data you hold and use, and why.** The ISBA website now contains a simple matrix for use by ISBA members. It is not intended to be a full turn-key solution but will be a helpful start in posing the necessary questions, including:
  - What information do you hold on individuals and where does it come from?
  - Do you share it with others, and for what reason?
  - Are parents, pupils and ex-pupils fully aware of what you are doing with their data and how much you hold? Indeed, can you answer that question honestly yourself?
  - Will your existing consents (e.g. parental or alumni consents) be valid under the GDPR, and are there other grounds apart from consent you could be relying on (e.g. legitimate interests, or fulfilling a contract or employment obligation)?

- **Identify any areas of potential vulnerability or gaps in your organisational knowledge**. Focus on these with the relevant people at the school first, which may help answer questions before you go to the expense of external advisers.

- **Table a review of your contracts, and keep up to speed with ISBA templates.** The effect of the new law will already be relevant on contracts covering the next academic year. This will include parent and staff contracts (if this is where certain consents are captured) and the wording of information collection forms (on pupils applying, joining, and leaving), as well as your contracts with third parties

If you have managed to instil good habits and introduce effective policies in your school to date, you will be well on the way to compliance

where there may be a data security aspect (IT services, hard copy and digital storage, even cleaning contractors – their position is changing under the new law too). Consider also where you are sharing data with third parties (for example your school's alumni organisation) or using a mailing house or cloud host. You will need to address this through data sharing agreements and/or data processing contracts.

- **The same applies to your policies review.** Although GDPR does bring specific new requirements for pupils, parents and staff, it goes beyond your data protection policy. Data protection also impacts on IT policies, CCTV, use of images, staff training, retention of records, and safeguarding / pastoral policies (namely in protocols for information sharing and reporting concerns). That is not to say that GDPR will make these jobs harder or more impractical – it should not. But it emphasises the need for joined-up thinking, especially given the additional rights being granted to individuals to control how schools use their data.

- **Conduct the need for a privacy impact assessment** before embarking on any new major projects or policy changes (say, a fundraising campaign, IT restructure or update to your privacy policy). This could be as simple as a meeting (properly minuted) or a short report, but GDPR says you must plan around privacy from the outset and evidence your decisions.

- **Get familiar with new or changing concepts:**
  - **Registration.** The legal requirement to register and notify your activities to the ICO on a central register will be abolished, but may be replaced by a levy.

- **Age.** We are awaiting final confirmation on the age at which GDPR confers rights of consent on children rather than their parents, but it is expected to be 13. At present, there is an unwritten rule that assumes an age of around 12, but this is subject to change depending on the maturity of the child. Language used in privacy policies and/or consents should therefore be clear and accessible for a child of 12 or older.

- **Liability of contractors.** For the first time, data processors such as cloud storage providers or web hosts will have direct obligations under the law. Your contracts with them will need updating and, as data controllers, you will need to ensure due diligence of your data processors.

- **Consent.** The rules on what constitutes legal consent (including for marketing) are getting tougher. The new ICO guidance due this summer will provide some answers, but remember that consent is not the only basis for processing data – indeed, under the new regime, it may not always be practical to rely on it. You may be able to show *compelling* legitimate interests instead as the legal basis for processing personal data, which means knowing (and telling people) what these reasons are from the outset – including in your privacy policies and other outward-facing wording.

- **New and expanded data subject rights.** We will not set these out in detail here, as this is one area where there is not much that can be done in the way of preparation – except in the general principle of knowing what you hold, and why, and whether it is lawful. Schools already used to dealing with intrusive data subject access requests will find these rights are supported by additional rights enabling a person to obtain an explanation of the ways in which his or her data is used, and (where you cannot justify it) object to this.

- **Transparency and accountability.** These buzzwords occur throughout the GDPR. Much fuller information is required from schools about what they do with data and what people can do to stop them. When challenged, by the ICO or individual data subjects (including staff, parents and pupils), the burden will lie with schools to demonstrate their compliance with the data protection principles.

This is already a lot for schools to take in, but specific updates on the ISBA website will be there to guide you through and the association will continue to work with partner organisations such as IDPE and legal experts to support you through this change.

Whilst each individual school must consider how they approach GDPR, based on their current data protection practices and how they process personal data of key stakeholders, please read on to see how some schools are preparing now for the changes to data protection.

Author
Owen O'Rorke
associate at Farrer & Co

T 020 3375 7348
W www.farrer.co.uk