COVER STORY

Stay GDPR-savvy

GDPR requires schools to keep internal records demonstrating **compliance and privacy**

Carry out **and document** a 'legitimate interests assessment'

Don't let GDPR creep up on you – **take positive action now**

The year of GDPR

The Bursar's Review has run a series of articles on preparation for the General Data Protection Regulation (GDPR) which takes effect on 25th May 2018. Here, we look back to the guidance given in the Summer and Autumn 2017 editions and consider where we are – specifically in respect of expected ICO Guidance and the latest on the new UK-only Data Protection Bill – and where we should be.

Hopefully, all schools will have by now appointed a compliance lead in this area – whether or not called a 'Data Protection Officer' (or DPO: see previous articles and ISBA guidance) – and begun both to raise awareness generally, and get support and buy-in from key staff and management. This ought to have precipitated an audit of whatever appropriate scale to understand what data the school holds, and why (both in the sense of 'for what purpose' and 'on what legal basis').

This step is recommended, and indeed we would say essential, before the school can meaningfully embark on the more tangible outputs of GDPR presentation, such as:

- **creating a new privacy notice** (incorporating new GDPR requirements in language appropriate to those it is aimed at);
- **reviewing all relevant policies where data protection has an impact:** data protection policy for staff (if separate), retention of records, CCTV / use of images, IT: acceptable use, etc;
- **considering the key contracts the school has that will be affected:** from parent contracts to subcontractors and outsourcing; and
- **reviewing forms and consent wording**, and indeed giving careful thought to where the school should seek to move away from 'consent-based' processing (and identifying where it cannot).

These are the outwardly-visible signs of compliance. However, GDPR also requires schools to have internal records demonstrating how compliance and privacy have been considered in major projects or risk areas, for example, fundraising, IT and safeguarding. The school ought to know how to carry out data 'privacy impact assessments' (PIAs or DPIAs) for these tricky areas, starting with a general one documenting the outcomes of the audit referred to above.

Until the school has carried out these internal assessments and identified where it is relying on grounds such as legitimate interests, rather than seeking consent, it is unlikely to bring much benefit for the school to attempt to draft any of its key policies, forms or the privacy notice itself.

To help schools in this lengthy process, ISBA (with Farrer & Co) is providing staggered guidance that was intended both to sit alongside the official guidance of the Information Commissioner's Office (ICO) and to fill in the gaps where we are still waiting for it.

GDPR preparation – what happened to the guidance from the information commissioner?

One of the key roles of the ICO is to produce intelligible guidance, both general and sector-specific, to assist organisations (and the public) in getting to grips with the complex and lengthy rules around data protection law. For data controllers such as independent schools, this generally means understanding where the line of compliance will be drawn in practice (and ideally, in good time before it takes effect).

In the past, one of the most common complaints about the ICO was the sheer weight and volume of their guidance, and its caution and specificity in interpreting the law – some would call it gold-plating. But in the build-up to GDPR, the opposite complaint has been heard: schools (in common with all sectors) have been crying out for final-form ICO guidance on key areas such as consent, legitimate interests, children, drafting PIAs, the appointment of a DPO and so on. However, despite some ever-expanding general guidance to the GDPR (accessible at W **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/**), the critical final form of the deep-drilling guidance in the key areas of most day-to-day impact is still outstanding in almost every area.

EU law

In fairness to the information commissioner, the blame for delay on this does not sit solely on her desk. For one thing, only a month after the final text of GDPR was agreed, the Brexit referendum threw the entire status of the legislation (temporarily) into doubt, and government support from the Department for Digital, Culture, Media & Sport (DCMS) – the sponsoring department – has been limited ever since. What is more, now that it is confirmed that UK law will have to reflect EU law on this issue, the ICO also needs to make its guidance consistent with that of the European Commission's relevant body (the Article 29 Working Party or WP29). This is also producing its own EU-wide guidance that adds to the body of useful, albeit wordy, material available for organisations.

For example, in December 2017, the WP29 finally produced its own draft guidance on consent for consultation – a full nine months after the ICO did the same. This is hopefully a step towards a settled version by the time this edition is published, or soon after.

Current guidance

The above should not fool anyone into thinking that the ICO does not have plenty of useful resources, for example:

- **Sector-specific guidance for education** is available on the ICO website, and the page W **https://ico.org.uk/for-organisations/education/** (containing a number of links and documents) was updated as recently as 21st December 2017. Inevitably, however, this is aimed across the board (rather than split into maintained schools, academies, MATs, free schools and independents) – and presents a mix of very general GDPR guidance, an hour-long webinar, and much more specific guidance relevant to schools that is still based on the Data Protection Act 1998. The latter is not a great deal of help when it comes to strategising over the (sometimes critical) finer points of GDPR, that said, many of the basic principles are not changing and schools should feel reasonably comfortable in adhering to such guidance as the ICO continues to publish until better GDPR guidance is available.
- **General guidance**, such as the evolving Guide to the GDPR document referenced above, is also conveniently linked from the above page alongside FAQs, step plans and self-help checklists. The most recent changes to the Guide to the GDPR (at time of going to press) were issued in December 2017, and key new or adapted sections cover the following areas:
- **Lawful basis for processing personal data**. Central to both current and new data protection law relies on the school establishing a 'lawful basis' for any processing of personal data. These include consent and 'legitimate interests' (see below). The ICO Guide emphasises the need to consider any existing or new processing and determine which lawful basis is met; and the new requirement to document and publish this in a privacy notice to be actively provided (wherever possible) to relevant individuals.
- **Consent.** As above, the ICO is still due to publish fuller guidance on GDPR consent, but the Guide (and the ICO draft – see below) gives a clear idea of its thinking; that GDPR sets a high bar. The ICO Guide reminds you to be clear that individuals can withdraw consent; and that if consent is withdrawn, you cannot then look for a different lawful basis. This makes it all the more important to consider what lawful means are available to process without consent, and the ICO Guide concedes that this is a legitimate approach.
- **Legitimate interests.** The Guide notes how flexible this very useful alternative to consent can be, but spells out that you need to:
  1. identify a legitimate interest for processing the data and set it out in your privacy notice;
  2. be able to show that your processing is necessary for that legitimate interest; and
  3. balance your interest against the privacy interests of the individual. It recommends that you carry out and document a 'legitimate interests assessment' for relevant processing activities and suggests an approach to this. Please note that legitimate interests alone will not be sufficient to process special category or criminal offence data; or to send electronic direct marketing.
- **Sensitive personal data** (now termed 'special category' and criminal conviction/offence data). In addition to a lawful basis, these categories of data (including information relating to race, religion, health and sex life) require you to meet a further, narrower, condition. Again, this must be documented and communicated to relevant individuals.
- **New subject rights** and how to comply with them W **(https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/)**

- **Documenting your efforts.** The Guide summarises here: **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/** the documentation schools should keep (1) to meet the direct requirements of GDPR and (2) to prove, as you may have to, that you are GDPR-compliant (for example, in obtaining consents, undertaking privacy impact assessments and providing privacy policy information). Data mapping/audit exercises will help as part of this exercise; all schools should be undertaking this as part of GDPR preparation, but such efforts must not end on or after 25th May 2018 – as compliance is an ongoing process.
- **Draft guidance on consent.** At the time of going to press, the ICO's draft consent guidance from March 2017 **(https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf)** remains the most detailed record of its intentions in this regard, and the longer WP29 draft (i.e. the EU Guidance) from December 2017 is available here: **https://iapp.org/media/pdf/resource_center/wp29_consent-12-12-17.pdf**. Both these contain some views on when consent is appropriate to obtain from a child, rather than a parent, in the meantime, ISBA has published its own guidance note on its website on consent as it applies specifically to schools, steering through this and other issues.
- **Brief guidance on privacy notices under GDPR**. (See **https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/**) and a relatively up-to-date, but more general privacy notice guide, which was drafted in 2016 but with trends towards GDPR in mind **https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/)**
- **A code of practice for drafting privacy impact assessments (https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/)** is now three years old but still has merit in its approach as a tool for GDPR compliance.

- **Draft guidance for consultation on the relationship between data controllers and data processors under GDPR W https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf)**. ISBA has also published materials on this in its online reference library at **W https://members.theisba.org.uk/53562**
- **A series of myth-busting blogs by the information commissioner W https://iconewsblog.org.uk/tag/gdprmyths/** do help cut through some of the scaremongering and misinformation, while reminding organisations that GDPR does mean change and a higher standard of data protection must be met. One reassuring message is that the ICO intends to use its new fining powers "judiciously and proportionately", and that its enforcement priority will be action against those who "systematically fail to comply with the law or completely disregard it, particularly when the public are exposed to significant data privacy risks". All good news for schools taking reasonable and proportionate care to comply with the new law (including, as above, documenting whatever steps are taken). However, advancement teams and alumni organisations may find this message hard to square with the fairly aggressive enforcement line taken on fundraising over the past two years.

What guidance is still to come?

In addition to the final consent and data processor guidance as above, the ICO has promised two further imminent guidance notes of particular relevance to schools; guidance on GDPR and Children, and guidance on legitimate interests (which many schools will be relying heavily on).

Looking beyond these, we still await a more granular, sector-specific view from the ICO on:

- who needs to appoint a DPO and whether this applies to non-academy independent schools (but as per previous articles, we are suggesting that such schools do not rush into the appointment before this is clear);
- a fully GDPR-focused guide to privacy notices and PIAs;
- updated GDPR guidance on the impactful area of subject access and fuller guidance on the other, new individual rights; and
- new guidance on direct marketing (with specific impact on the area of fundraising).

Fundraising

The Direct Marketing Association and the Fundraising Regulator have each published guidance on areas such as:

- legitimate interests, at: **https://dma.org.uk/uploads/misc/59ca0f2e17ef3-dpn-li-guidance-publication_59ca0f2e17e5a.pdf** and
- consent, at **https://www.fundraisingregulator.org.uk/information-registration-for-fundraisers/guidance/personal-information-fundraising-consent-purpose-transparency/**

Although beyond these two specific issues, the rules around direct marketing are not materially affected by GDPR. Instead, a new ePrivacy Regulation will replace the Privacy and Electronic Communications Regulations (PECR) rules, probably from some time in 2019, and it is unlikely new guidance will arrive before then. However, the ISBA is also publishing its own fundraising toolkit of materials this spring.

What to look out for

As mentioned above, the new ePrivacy Regulation will have a particular impact on telephone and email direct marketing (including fundraising), use of social media, and website cookies. It is still being negotiated in Brussels. Finalisation of the new law is lagging some way behind GDPR – but the schools (or alumni organisations, as applicable) are likely to have at least a year to digest the new rules, once agreed, before they take effect.

Finally, a new UK-only Data Protection Act will sit alongside GDPR and, broadly speaking, plug the gaps left by the EU for member states to fill in on a domestic basis (including the age of children to consent to online services – which will almost certainly be 13, but please be aware that this is not a universal rule for all types of consent given by children).

The bad news is that the first draft of this (September's Data Protection Bill 2017) ran to 194 clauses; and even at the time of publication it is some way off being agreed in parliament, even though it must come into force in May 2018. The better news is that, very broadly, the Government is looking to plug those GDPR gaps by mirroring existing data protection law quite closely.

Take positive action now

We trust that this article will serve as a run-through of what official resources are available to schools, alongside those provided by ISBA. The key message to those who are not as far along as they might have hoped remains not to panic, but to take positive action rather than let GDPR creep up on you. The ICO will not be rushing to use its enforcement powers but it is likely to pick out the easiest targets in each sector – often those in respect of whom it receives the most complaints. The best advice is to ensure your school is not one of those easy targets, and that – in the event that any complaints are made – you are able to show good, informed understanding of the law and good record-keeping of its compliance project.

The above guidance is part of that, but it is no more than a tool to achieve a better corporate, cultural understanding of the issues as they relate to your school. Ultimately, to be successful and sustainable, compliance must be led by knowledge from within.

Author
Owen O'Rorke
associate at Farrer & Co

020 3375 7348

This article is intended as a general guide to the area and an update on key developments in current guidance and thinking. Neither this article nor any guidance referenced within it is a substitute either for specific legal advice, or full internal assessments to be carried out within your school.