The IDPE has worked in association with ISBA and Farrer & Co on the following guidance note.

December 2017

IDPE recognises the importance of working across the school to become GDPR-ready, and therefore this template guidance covers all areas relating to data controllers, data processors and data sharing agreements, reflecting the need for a whole-school approach to GDPR. However, to make your life easier we have highlighted in blue which sections of this guidance are most relevant to schools' development professionals.

What is a Data Controller?

Independent schools are, for the purposes of data protection law (both now and when GDPR comes into force), "Data Controllers" of various personal information – for example, relating to staff, pupils and parents, past, present and prospective – that they hold and determine how to use. Although we refer to those uses as ways of "processing" personal data, there is a specific and separate legal meaning attributed to the term "Data Processor".

What is a Data Processor?

This means any person, company or body that processes personal data on behalf of a Data Controller (i.e. another person, company or body who has provided them with certain personal data for a specific purpose). While it is in the Data Processor's hands, the personal data in question remains, in broad terms, the responsibility of the Data Controller. That remains the case under GDPR, although GDPR will mean that Data Processors will have certain liabilities and obligations *in addition to* the liability that remains with the Data Controller.

This relationship is reflected – and indeed, as a legal requirement, must be accurately captured – in the written contract between the two: the data processing agreement. That will determine the extent and scope of the Data Processor's instructions in how it can use the personal data, most obviously to perform a service for the Data Controller.

The data processing agreement must also, as a legal requirement under GDPR, cover off issues like the security of the data, record keeping obligations, breach reporting, returning or destroying the data on command, and limitations on sub-contracting (or rather "sub-processing") – meaning that a sub-contractor cannot be appointed to process the personal data without the ultimate Data Controller's knowledge and permission.

Subject access requests (and similar rights) exercised as against a data processor should be passed on to the Data Controller to deal with, although the data processing agreement

should make provision for how to handle this (including assistance from and delegation to the Data Processor where appropriate).

There is an advantage to all this, which is that provided that the Data Controller itself (the school in this context) has a lawful reason to process the data, it does not need to find an additional lawful basis or "condition" to provide that data to a third party – even if the personal data is sensitive / "special category" data – as long as if that third party is, truly, its Data Processor. Nor does the school have to inform its data subjects (e.g. the school community) as to whom its Data Processors are. That is because, in this narrow and protected context, it is not considered "sharing" of data with a third party. Provided the arrangement is supported by a clear and compliant contract, the law views it much as if that Data Processor were the school's employee, or simply a temporary extension of the Data Controller: after all, provided the data processor agreement terms are properly observed, the data never leaves the school's "control".

There are, however, certain specific rules which are covered in the data processing agreement, and this guidance note.

What does this mean in practice for us?

So far, this may all sound very theoretical and dry. However, it may begin to make more sense in the context of actual service contracts that a school might enter into. Notably:

- **Pension plan** or **payroll** providers for staff;

- **IT service contracts**: these are the most commonly-seen, and perhaps the most obvious, forms of data processor agreement. A major consideration with IT / software contracts is whether any personal data is being transferred outside the EEA (e.g. for storage by a technology firm in the US) and, if so, on what lawful basis and with what safeguards.

    Examples applicable to schools might be **cloud storage providers** who host files and databases for schools; **website or intranet designers** who handle images and data for the purposes of online resources; **monitoring systems / eSafety providers** who may (depending on the nature of the set-up) have some oversight of personal data on the school system; and **external IT consultants** who may from time to time have access to school systems and devices to perform checks or maintenance.

    However, while IT providers may be most used to signing agreements of this nature, they may also have their own standard terms that they will seek to impose. Schools should be prepared to check and negotiate these as they may not have had due diligence paid, or been updated for GDPR; or if they are updated, the service provider may have included more favourable terms for themselves (e.g. higher fees or better indemnities) to reflect the increased level of legal liabilities for Data Processors under GDPR.

- **Security firms** who may (depending on the set-up) run **biometrics** or **CCTV systems** on behalf of the school, or **secure disposal** of documents;

- Other forms of **service contract**, including **catering**, or those running **school trips** or **external courses**. In some cases, the personal data here will only form a small part of the service, but it may be important – and it may be sensitive ("special category") data. For example, caterers will need to know staff and pupil allergies (by name); those handling external trips and courses will likewise need to know certain medical data.

- **Marketing agencies** (e.g. MailChimp), **fundraising consultants**, **wealth screening companies**, **data appending companies** (e.g. for matching telephone numbers to addresses). These require special consideration of what third parties are entitled to do with what data, and who is the data controller.

- **Other individual consultants**. These may include:

    - peripatetic staff / sports coaches / music teachers: such staff should be under standard contracts with the school, but such contracts are likely to require data processing clauses (such as those short-form clauses proposed for insertion); and

    - specialists such as safeguarding consultants or experts brought in to review or assess an incident or question of culture. Such people will have access to highly significant and often sensitive ("special category") data. It is common practice to require a statement of work and confidentiality (non-disclosure) agreement, but ideally this should be combined with a data processing agreement.

How to use the data processing agreement

We have provided two alternative approaches:
(i) a longer data processing agreement (that may be stand-alone or attached as an Annex or Schedule to e.g. an IT service agreement)
(ii) a shorter series of clauses that should be included, or closely mirrored, in other forms of standard agreement (e.g. a catering contract) where there is a narrow but important need for (personal data to be processed)

Standard agreements for coaches, music teachers or temporary staff should be reviewed to ensure the data processing clauses mirror these in content, albeit that the wording will need tailoring to reflect the actual responsibilities of the staff concerned.

It is worth being specific in each contract (whichever form is used) what categories of personal data are likely to be processed on the school's behalf under the contract, especially where the data is sensitive / "special category".

Whatever the subject matter of the data processing agreement, the technical law involved does require a fair amount of jargon and "boilerplate" clauses – which is why we hope these GDPR-standard templates, prepared along with this guidance by Farrer & Co, will be of wide application. However, each scenario will have its own unique issues and data uses, and the templates should not be used without the benefit of individual thought and adaptation to the situation. Legal advice should be sought in case of any doubt.

The two different documents (stand-alone and "insert" clauses) reflect the fact that in some cases above (e.g. database storage), data processing is a core activity connected with the service – whereas for some (e.g. catering), it is an ancillary aspect. It is also the case that sometimes the school will be contracting with a company, and sometimes an individual. However, in data processing terms, the law views the relationship as fundamentally the same.

How is GDPR changing things?

As well as imposing liabilities (and reporting obligations) on Data Processors for data security breaches, as well as record-keeping duties and (in some cases) the obligation to appoint a Data Protection Officer, GDPR materially increases what needs to go into a data processing agreement.

In reality, most schools without legal officers or (within the GDPR meaning) Data Protection Officers will not be expected to be completely familiar with the ins and outs of Article 28 GDPR that sets out what needs to go into a data processing agreement – but either that, or these documents, should form a checklist in the event that the school is presented with a data processing agreement by a third party who refuses to accept the school's template.

If they refuse to accept any sort of compliant data processing agreement, however, they are putting both parties at risk of processing unlawfully. The law (or ICO) may either view it as unlawful processing because of the lack of written instructions and legal safeguards; or alternatively, without formal contractual limitations on what the Data Processor is allowed to do, the activity may simply be seen as an unlawful act of data sharing with a third party, without the protections of a "data processing" arrangement.

Equally important for schools is to identify what existing data processing agreements they have in place that are either inadequate (or missing) now, and which extend in term beyond 25 May 2018 – as it is likely these will need to be reworded (i.e. amended or varied) or novated / terminated and renegotiated. As suggested above, some renegotiations may be led by Data Processors themselves, who will be expecting preferable terms or concessions.

Schools are therefore recommended to take the lead where they can, using GDPR as a lever, to impose preferred terms – and to check whether they are entitled to terminate their existing arrangements if they have cause to believe that to continue without amendment would place the school potentially in breach of data protection law.

How do I know if this is a Data Processor situation, and who is the Data Processor?

This is a very good question, and it will not always be obvious. This particular construct of law does not lend itself perfectly to every situation, including with schools. The best approach is to consider from first principles:

(i) Do we need to provide any of our personal data to this person / company for them to do the job?
(ii) If so, do we want it back? Do we expect to stay in control of it? Is it unnecessary for the third party make any decisions in their own right about how to use it? (Apart from purely technical decisions, or decisions within the scope of our instructions)
(iii) If so, then this is likely to be a data processing agreement. If not, then the third party is likely to be a data controller in its own right, and the school will have to consider whether it has some other lawful basis that makes it necessary to share – or if a formal data sharing agreement is the way to go.

The situation can be complicated by scenarios where an agreement requires a party to be Data Processor in some respects (or in respect of some data), and Data Controller in others. For example, a **wealth screening consultant** will hold certain data on individuals as a data controller, but will only use the data you provide it for specific purposes (and should not otherwise keep it).

Another anomaly would be **external markers / examination boards**, who will process some pupil data on the school's behalf (including examination scripts and returning results) but may also be data controllers in their own right, recording marks, processes and appeals with independence. A stand-alone agreement of the nature attached is unlikely to be practically applicable in such situations, but data processing issues – and deciding where responsibility for e.g. responding to subject access lies – should be considered and agreed.

In other situations, two organisations may both be data controllers, independently, of the same data pool (and have separate rights in the same); or be "joint data controllers" of the same data (which means they are jointly liable but need to decide, contractually, between themselves who is entitled to do what with that data). These are not always black-and-white decisions, and need careful thought to get right in order to: (a) choose what legal arrangement best suits the school; and (b) make sure the agreement reflects the reality, and vice versa.

This is particularly relevant in scenarios where schools have separate **alumni organisations**, and separate legal advice is always recommended (although these issues will be dealt with in the forthcoming Fundraising Toolkit).