Preparing for the General Data Protection Regulation (GDPR) – 10 Steps for Schools

Introduction

This checklist sets out 10 preliminary steps that schools can now take to prepare for the EU General Data Protection Regulation (GDPR) which comes into force in the UK on 25 May 2018.

When the GDPR comes into force, it will entirely replace our current Data Protection Act 1998 (DPA) and radically overhaul many of our existing data protection rules. Some of the precise detail as to how the GDPR will be implemented here in the UK has yet to be decided. So, whilst this checklist is a useful starting point, you should continue to check the Information Commissioner's Office (ICO) website (www.ico.org.uk) for further guidance and other tools to help you prepare.

You should also refer to the ICO's 12 Steps Checklist available at:

https://dpreformdotorgdotuk.files.wordpress.com/2016/03/preparing-for-the-gdpr-12-steps.pdf

Step 1 – Raise Awareness

Key decision makers in the school need to know that data protection law is changing and how those changes will affect how the school is run.

Key decision makers will therefore need to familiarise themselves with the GDPR now, and identify areas where the school will need to make changes in order to be compliant.

GDPR will have significant resource implications (in terms of both budget and staff time) so this fact should be quickly communicated to senior management and governors quickly so that arrangements can be put in place. We recommend that you use the lead-in period to get ready and raise awareness of the upcoming changes.

If your school has a Data Protection Officer (DPO), they may wish to lead this process. If you have yet to appoint or designate responsibility for data protection, we recommend that you do so now because the GDPR will impose significant additional compliance burdens. For some schools, the designation of a DPO will become a mandatory requirement in any event.

It is important to emphasise that the scale of the work is such that your DPO is likely to need support, perhaps from an Information Governance team which includes representation from key functions within school, including ICT. Some of this is likely to be influenced by the size and functions of your school.

Step 2 – Accountability and Data Governance

One of the main features of the GDPR is that compliance alone is not enough; data controllers will also have to demonstrate their compliance and prove that they are taking data protection

seriously by implementing a range of accountability measures. These measures include Privacy Impact Assessments, data protection audits, policy reviews, activity records, and in some cases (such as academies), the mandatory appointment of a DPO.

Here is an overview of some of the accountability measures you will need to understand:

Privacy Impact Assessments

Privacy Impact Assessments (PIA) are not new, but what is new is that the GDPR will expect them to be undertaken in certain cases. PIAs will need to be carried out when you are planning a new initiative which involves "high risk" data processing activities i.e. where there is a high risk that an individual's right to privacy may be infringed, such as monitoring individuals, systematic evaluations, or processing special categories of personal data, especially if those initiatives involve large numbers of individuals or new technologies such as biometrics.

The idea behind a PIA is to identify and minimise non-compliance risks.

The ICO has produced a Code of Practice on PIAs which will help guide you through the process.

Pseudonymisation (Pseudo anonymisation)

This new term refers to the technique of processing personal data in such a way that it can no longer be attributed to a particular data subject without cross referencing it with other further information. The aim here is to be able to collect and use data relating to an individual without having to know that individual's identity. For example replacing fields containing a pupil's name and / or pupil number with a pseudonym. The further information must be kept separate and subject to technical and organisational security measures so as to ensure that the data subject cannot be identified.

Pseudonomised information is still a form of personal data, but the GDPR promotes its usage in certain circumstances in order to enhance privacy and contribute to overall compliance.

For example, GDPR may expect pseudonymisation to be considered when personal data is processed in a way which is "incompatible" with the purposes for which it was originally obtained. Alternatively, the technique could be appropriate for schools wishing to use pupil data for historical or statistical purposes.

Data Protection Audits

We would suggest that schools should review and document the personal data they hold, identify the source, who it is shared with and the legal basis upon which they rely in order to process the data. This exercise is commonly called a data protection audit and can be deployed across the entire school, or confined to distinct areas within it. Unless you know what personal data you hold and how it is being processed, it will be difficult to comply with the GDPR's accountability principles which require you to be able to demonstrate how the school complies with the data protection principles in practice.

Another critical benefit of a data protection audit is that it maps the flow of personal data into and out of the school, and can be used to measure the degree to which the school complies with the law and identify "red flags" which require urgent attention.

Some schools may not have thought about the legal basis for processing personal data, and under the DPA this didn't have any particular consequences. However, under GDPR, all data controllers will have to identify and document the legal basis for each processing operation.

Article 6(1) GDPR lists a range of grounds for processing personal data which are very similar to the grounds listed in Schedule 2 of the DPA. They include, amongst other things, consent of the data subject, necessary for a contract with the data subject and necessary for the purposes of the legitimate interests of the data controller.

Identifying the school's legal ground for processing personal data is not a step that can be avoided without consequences. This is because GDPR expects you to explain your legal ground for processing personal data in your Privacy Notice issued to parents, pupils and staff and also when you respond to any Subject Access Request (SAR). In addition, depending on the legal ground for processing personal data, there may be implications for individuals' rights. For example, if the school relies upon parental consent in order to use images of pupils on the school website, parents will have a stronger right to have the data deleted.

We have particular expertise in carrying out data protection audits in schools, so if your school needs help with this, please get in touch.

Data Protection Policy Reviews

The GDPR is likely to require all schools to review their policies, particularly those relating to data protection. Data protection policies for pupils and parents are used to explain an individual's legal rights and how those rights can be exercised. Because the GDPR amends those rights, your policies will also have to be amended.

Any policies also intended to be read by children will have to be explained in clear non-technical language and in a way that can be readily understood by the intended audience.

You should ensure that your policies are easily accessible and not "buried" on your website.

Appointment of a Data Protection Officer (DPO)

Due to the significant new burdens imposed on data controllers by GDPR, we recommend that all schools now formally appoint a DPO. Most schools have in fact already done this because of the demands of the existing Data Protection Act.

Under GDPR, certain data controllers and data processors *must* appoint a DPO. These include:

- Public authorities (with some minor exceptions) – this means that all maintained schools and academies will have to mandatorily designate a DPO.

- Any organisation whose core activities require *"regular and systematic monitoring"* of data subjects on a *"large scale"*; or *"large scale"* processing of personal data or criminal records.

At this stage, it is not clear if an independent school will have to appoint a DPO or not. In any event, member states are at liberty to pass further legislation identifying other data controllers that must designate a DPO. That said, our strong view is that all independent schools should appoint one in any event because of the significant tasks required to comply with both existing data protection law and the forthcoming GDPR. Your DPO should receive enhanced DPO training. If you would like Harrison Clark Rickerbys to deliver GDPR training for key staff and / or data protection for all staff, please contact us to discuss your requirements.

Where a DPO is appointed (whether that be on a mandatory or voluntary basis) the DPO then becomes responsible for all of the data processing activities carried out by the school. This

means that it won't be possible to circumscribe the scope of the DPO's dominion by only allowing him or her access to certain areas.

In addition, where a DPO is appointed (whether that be on a mandatory or voluntary basis), Articles 37-39 of GDPR will apply to their appointment. Articles 37-39 of GDPR set out very specific requirements covering the type of person that should be appointed and their responsibilities. Such as:

- **Knowledge and Support**: The DPO should be an expert in their field *and* have specific knowledge of their sector. The employer must help them maintain this knowledge e.g. by making provision for specific training.

- **The DPO's tasks** should as a minimum include: advising colleagues and monitoring the school's compliance via staff training and awareness raising; advising on PIAs; being the point of contact for supervisory authorities; developing policies and procedures; watching out for publication of relevant guidance and Codes of Practice; monitoring the documentation, notification and communication of data breaches.

- A DPO can be an **employee or a hired contractor.**

- **DPO's must be able to work *"independently of instruction"*** and not be dismissed or penalised simply for doing their job. They should report to the highest level of management. This requirement will have interesting implications from an HR perspective.

  Conflicts of Interest: Another noteworthy point is that whilst the GDPR doesn't prohibit the DPO from holding other posts within the organisation, it does stipulate that conflicts of interest for the DPO are to be avoided.

  A somewhat more prescriptive and hard-line stance has been adopted by the Article 29 Working Party (A29WP) in their recent Guidance on DPOs. *(The Article 29 Working Party is a group that is represented by the data protection authority from each of the 28 member states of the EU, the European Commission and the European Data Protection Supervisor.)* The A29WP Guidance can be read here http://ec.europa.eu/newsroom/document.cfm?doc_id=43823

  Two scenarios which are likely to generate conflict of interests include: where the DPO is appointed internally from senior management (e.g. Head of HR or Head of IT) or if the appointment was from someone holding a lower role within the organisation, if their role involved them determining the purposes and means of processing personal data.

  Secondly, even certain external DPO appointments could create a conflict of interest e.g. where the external DPO is a lawyer providing day-to-day data protection support to the data controller or processor.

- The DPO's **contact details must be published** and registered with the supervisory authority. They will be the point of contact for compliance matters.

- **Under the GDPR the DPO is not in charge of maintaining records of processing activities.** However, the A29WP Guidance provides that nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the records of processing operations under the responsibility of the controller or the processor. The Guidance further provides that such records could in fact be considered to be an important tool in assisting the DPO to perform his or her tasks of informing

and advising the controller or the processor, and monitoring compliance with the Regulation.

Staff Data Protection Training

Schools will continue to be subject to an obligation to take organisational steps to keep personal data secure and the deployment of staff data protection training will continue to be expected. New starters should receive data protection training before they have access to personal data and existing staff should receive regular and refresher training.

Schools that breach the GDPR (or the current DPA), will be criticised if they have failed to ensure that all staff that handle personal data have received data protection training. This is because staff training is a simple organisational measure that an organisation can take to reduce the likelihood of data losses.

To Do List

- Don't wait for GDPR to come into force to train your staff in data protection. All staff that have access to personal data should receive mandatory basic data protection training and key staff that need to know more should get enhanced training. Keep records of who has received training and when and ensure that those staff who didn't attend (for whatever reason), get trained as well.

- If you have yet to do so, appoint a Data Protection Officer now. Watch out for guidance from the ICO as to any restrictions on the appointment.

- Carry out a data protection audit so you have a map of your personal data flow already in place when GDPR goes live.

Step 3 – Communicating Data Protection/Privacy Information

GDPR requires you to provide much more meaningful information to individuals about how you use their data.

Under the current DPA, schools are already legally required to provide certain minimum information to individuals (including staff, pupils and parents) about how their personal data is processed. This is commonly provided through a Privacy Notice which may or may not be incorporated into the school's Data Protection Policy.

Under GDPR, the list of information which has to be provided to individuals will increase significantly. Some of the information has to be communicated in all cases (mandatory Privacy Notice information) whilst a second subset of information need only be provided in specific cases e.g. if the school intends to process the personal data for further different purposes than those that existed at the time of collection. Notwithstanding the sheer volume of information that now needs to be included in your Privacy Notice, you will be expected to provide this in a concise, transparent, intelligible and easily accessible way (which will be particularly important when aimed at children (see Step 9 below). Here is some of the information you will be expected to provide:

- Your identity and contact details

- The purpose of processing their data and the legal basis for the processing of that data (This latter requirement is new and will require significant thought in some cases)

- Who you share the personal data with
- Transfers outside the EU and how data is protected
- Retention period or criteria used to set this
- Tell individuals all their legal rights e.g. the right to withdraw their consent to their data being used for marketing or for school fundraising
- Right to complain

To Do List

Your DPO should review your existing Privacy Notices and update them so they comply with the GDPR. Be sure to capture all of your existing Privacy Notices and be mindful that they can appear in different and disparate places e.g. embedded within your Data Protection Policy, Terms and Conditions of the Parent Contract, or on the Admissions paperwork or website.

Ensure that any changes you make to your policies and privacy notices remain consistent with what you say in your Terms and Conditions of the Parent Contract.

The ICO has now published its new Code of Practice on Privacy Notices and because it takes into account the new GDPR requirements, you should refer to it when crafting your new Privacy Notices. It can be viewed here https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

Step 4 – Legal Grounds for Processing Personal Data

GDPR sets out conditions (or grounds) that must be met for the processing of personal data to be lawful. These grounds broadly replicate those in the current DPA. For example, personal data may be processed with consent or where the processing is necessary for a contract or where the processing is necessary for compliance with a legal obligation.

Most organisations, including schools, may not have had cause to think about their legal basis for processing personal data before. This is largely because under the current DPA there are very few circumstances where this is relevant. However, under GDPR you will need to know your legal grounds for processing personal data and in some cases explain it to your pupils and parents. For example, it is likely that your legal ground for processing pupil images for identification purposes will be because the processing is necessary for the contract. In contrast, the legal ground for using pupil images for school marketing and on the school website is likely to be consent.

You will have to explain your legal grounds for processing personal data in your Privacy Notice or when answering a SAR. This is new.

In addition, under the GDPR, some individuals' rights are modified depending on your legal basis for processing their personal data. For example, individuals will have a stronger right to have their data deleted where you use consent as your legal basis for processing.

To Do List

The school should look at the different types of data processing it carries out and identify and document the legal basis for carrying it out via data protection audit or data mapping exercise. Documenting this will help you comply with the GDPR's accountability requirements. This information is part and parcel of any good data protection audit.

Step 5 – Consent

The school should review how it seeks and records consent for the processing of personal data and consider if any changes are required under the GDPR.

Just as with the current DPA, schools can still rely on "consent" as a legal ground to process personal data e.g. to use pupil images on the website, to send fundraising and marketing messages to parents and Alumni, or to publish pupil news on social networking platforms. However, satisfying the criteria for valid legal consent will be harder under GDPR than under current law.

Schools should have particular regard to recent enforcement activity in the charity sector where existing data protection rules are being more robustly enforced by the ICO in respect of direct marketing. School Development Directors should review their existing development activity and in particular the DPA requirement in Principle 1 of the DPA to process personal data fairly so as to ensure that whatever development activity is undertaken it is suitably transparent. This requirement to process personal data fairly is engaged even where consent is not relied upon as a legal ground to process personal data. For example, you may be able to legitimise the processing of personal data for school development purposes on the ground that the activity is in the "legitimate interests" of the school. Even where this is the case, you are still required to provide individuals with sufficient information about the activity in order to meet fair processing requirements. The more intrusive the activity is, the harder it will become to rely upon the "legitimate interests" ground and more detail will be required in your fair processing information.

Under GDPR, consent of a data subject means ***any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to personal data relating to him or her being processed.***

- **Freely given:** The consent must be freely given and capable of being withdrawn at any time. It must be as easy for an individual to withdraw their consent as it was to provide it in the first place.

  "By signing this contract you are also consenting to…"

Where the performance of the Parent Contract is made conditional on consent to the processing of personal data that is not necessary for the performance of that contract, this is likely to result in consent not being freely given.

Specific: Separate consents must be obtained for different processing operations. It must be distinguishable from other matters and not "buried" in wider written agreements. Under GDPR there is a presumption that consents should be separable from other written agreements. (This could require attention since many standard parent contracts incorporate consents for a multitude of other processing activities, such as marketing. Schools should therefore be prepared to separate processing activities which are based upon and require consent from those which are actually based upon contractual necessity.) Under GDPR it will become necessary to provide parents and pupils with more granularity of choice so that they have the ability to consent separately to different types of processing wherever possible. For example, under GDPR it would be appropriate to separate consent for use of images on the website to use of images in the School Prospectus. This new demand for granularity may cause some difficulty for those schools who currently are only able to manage consent on a "one size fits all" basis.

- **Fully informed:** You should clearly explain to individuals what they are consenting to and of their right to withdraw consent.

- **Consent must be unambiguous and be a positive indication of agreement:** It cannot be inferred from silence, inactivity or pre-ticked boxes.

To Do List

- Review the school's terms and conditions of the Parent Contract, Acceptance Forms and Consent Forms so they meet the higher standards of GDPR.

- Abandon the use of pre-ticked, opt-in boxes, and carefully consider use of opt-out boxes to ensure they comply with GDPR. The use of the opt-in box is far more likely to result in GDPR compliance.

- Get clear consent for the different uses of personal data. Don't "bundle-up" or "bury" consents within broader contracts.

- GDPR requires you to demonstrate that consent has been given. Review your systems for recording consent to ensure you have an effective audit trail.

The ICO has recently published its draft new Guidance on Consent to help you decide when it is appropriate to rely upon consent as a legal ground for processing personal data and when it would be appropriate to rely upon an alternative legal ground. It also explains what counts as valid consent and what practical steps you can deploy to help you record and manage consents in a way that is GDPR compliant. The consultation period for this document has now ended but a copy of the draft guidance is still available here. https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

Step 6 – Individuals' Rights

The legal rights that individuals have under GDPR are very similar to those they currently enjoy under the DPA. However, there are some significant enhancements and amendments which you need to be aware of.

The main legal rights under the GDPR include:

- **The right of subject access** (see below)

- **To have inaccuracies corrected**

- **To have information erased** (the so called "right to be forgotten")

- **To prevent direct marketing** (i.e. where marketing is directed to specific individuals)

- **To prevent automated decision-making and profiling**, and

- **Data portability** (This is a new enhancement to the right of subject access. In brief, schools will have to provide requested information electronically and in a commonly-used machine readable format.)

The A29WP has already published its Guidelines on the individual right to data portability. It can be viewed here
http://ec.europa.eu/newsroom/document.cfm?doc_id=43823

Step 7 – Right of Subject Access

As under current data protection law, GDPR will continue to allow individuals to ask the school to give them a copy of their personal data together with other information about how it's being processed by the school. (This is known as an SAR).

However, under GDPR the rules for handling SARs will change and the school will need to update its procedures accordingly and plan for how it will meet the new deadlines and other new requirements.

Under GDPR, the main changes are:

- Now free in most (but not all) cases (used to be £10)
- Manifestly unfounded or excessive requests can now be charged for or refused
- Deadline reduced from 40 calendar days to "within 1 month". This deadline can be extended in certain cases.
- Additional information to be supplied e.g. school data retention periods and the right to have inaccurate data corrected.
- If you want to refuse an SAR, you will need to have policies and procedures in place to demonstrate why refusal of a request meets these criteria.

Step 8 – Personal Data Breaches

All schools will have to adopt internal procedures for detecting, reporting and investigating a personal data breach.

The reason for this is that GDPR introduces mandatory breach notification to the Data Protection Authority (the ICO) and in some cases also to affected individuals. Only those breaches which are likely to result in an individual suffering damage will need to be reported e.g. breaches that could result in identity theft or where an individual's confidentiality has been breached. However, even though not all breaches will be subject to mandatory notification, you will still be under an obligation to have systems in place to detect and investigate all breaches. You should also maintain an internal breach register.

Where the school detects a breach which is subject to the mandatory reporting rules, then it must report the breach to the supervisory authority without "undue delay" and not later than 72 hours after becoming aware of it. This in itself could pose significant challenges given that it can take organisations several hours or even days to identify where the breach took place, which individuals have been affected and the data that has been compromised.

Where a breach has to be reported to affected individuals this will have to be done without "undue delay".

Non-compliance can lead to administrative fines of up to €10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover or the preceding financial year, whichever is higher.

Step 9 – Children

The GDPR identifies children as "vulnerable individuals" deserving of "special protection". To that end, you need to be aware that the new rules introduce some child-specific provisions, most notably in the context of legal notices and the legal grounds for processing children's data.

You should also look out for Codes of Conduct, which are likely to be published which may further restrict the way in which children's personal data can be processed. Schools should therefore carefully consider whether the new children-specific rules are likely to affect them and amend their processes in order to comply with the GDPR rules.

The GDPR do not prescribe the age at which a person is a child and in this context, all schools will need to address the new requirements when writing notices aimed at teenagers and young adults. In any event, any legal notice addressed to a child (whether relating to online or off line services) must be child-friendly.

The main provision in respect of children is that where information society services* (e.g. the sale of certain goods and services online) are offered directly to a child and the legal ground for processing personal data is consent, then parental consent will be required for children aged under 16. This threshold can also be lowered to 13 by a Member State.

*'Information society services' includes most internet services provided at the user's request and for remuneration. In its guidance, the ICO states that GDPR emphasises that protection is particularly significant where children's personal information is used for the purposes of marketing and creating online profiles.

Ultimately though, under 13's can never themselves consent to the processing of their personal data in relation to online services. This rule is subject to certain exceptions such as counselling services.

The school as data controller would also be required to make reasonable efforts to verify that consent had been provided.

Offline processing of personal data will continue to be subject to the usual Member State rules on capacity to consent.

Step 10 – International Data Transfers

Under current data protection law, transfers of personal data outside the European Economic Area (EEA) are restricted and this will continue to be the case under GDPR. In general terms, the rules on data transfers under GDPR are very similar to those under the DPA with some improvements.

Schools should review and map any flow of personal data outside the EEA, consider what transfer mechanisms are in place and whether these comply with GDPR or not.

Most schools do send personal data outside the EEA, whether through the use of service providers such as Cloud Service Providers, bulk emailing services, web hosting services or simply communicating with parents or agents overseas.

If you have been sending personal data to the US and relying on the US Safe Harbor scheme, which was previously approved by the European Commission as providing an adequate safeguard for the transfer, this is no longer valid. Discussions to replace Safe Harbor with EU-US Privacy Shield are, at the time of writing, ongoing.

The GDPR will continue to offer existing methods of transferring personal data. For example, standard model contract clauses which have been approved by the EU Commission and adopted by a Member States supervisory authority will remain a practical option for most types of transfers and the existing sets of clauses will remain in force. There will also continue to be a set of derogations (exemptions) which will permit the transfer of personal data under certain circumstances e.g. explicit consent and contractual necessity etc.

Breach of the GDPR's rules on data transfers will be subject to maximum level fines of up to 4% of worldwide annual turnover.

Further Assistance

If you require any assistance with preparing for the GDPR, staff data protection training (including School Data Protection Officer specific training) or data protection legal advice please contact:

Paula Williamson, Consultant Solicitor at Harrison Clark Rickerbys, 01242 246405 or pwilliamson@hcrlaw.com.