

Clare Atkinson is a Trustee of IDPE (Institute of Development Professionals in Education) and also Development Director at Dr Challoner's Grammar School, Amersham. Here, she answers some very specific questions from FundEd magazine, around the practicalities of implementing GDPR in relation to fundraising and community engagement activities:

Q - Universities enjoy significant support from their alumni and FundEd encourages schools to do the same. On what basis can schools ask for contact information from students who are leaving?

A - For some time, we have been seeking permission from our alumni to keep in touch with them after they have left. We send newsletters, fundraising information and encourage them to come back to help with our careers events or place adverts in the school magazine. The legal basis for collecting this information is legitimate interest. However, it is crucial that schools do not fall foul of the Privacy and Electronic Communications Regulations (PECR) legislation and ensure that permission is sought for electronic communications such as email, SMS or telephone calls to numbers registered with the Telephone Preference Service (TPS). We would not contact a student without this consent; it would be counterproductive and potentially damaging. We have very few students who ask not to be contacted once they leave the school and we, of course, respect their wishes. Often, students will then renew contact at a time that suits them to do so.

The ICO have indicated that doing this is acceptable although schools should continue to review their lawful basis for processing and ensure legitimate interest to contact your alumni remains valid. The school must be explicit in their privacy notice as to the reason why they are collecting any information and what they will be using that data for, and you will need to have a retention policy which clearly states how long you keep your data for. It is also important to ensure that communications are managed so as not to bombard an alum. We want to build long lasting relationships rather than something short term.

Q - Are there any restrictions on contacting local businesses to request support i.e. for sponsorship/careers workshops. How should this data list be maintained?

A - No, as long as the request relates to the actual business (rather than a request for personal support from the individual). With local businesses, you are more likely to be successful by asking someone from the school community to make this approach - a parent or governor - particularly if they have an existing relationship with the business. Our recent careers fair had many parents involved. We ask them for support and then they contact us if they can help. Of course, such information should then only be kept for as long as necessary – i.e. whilst planning and executing the event. Exhibitors could however, be asked if they would be interested in helping again in the future, which would justify keeping such information for a longer period of time with this specific purpose in mind.

Q - Is it acceptable to maintain a database of local clubs – both those that have used or currently use the school's facilities and those who don't (but might want to)?

A - Yes, as long as the information stored is not personal data. If it is personal data i.e. a personal email address for the contact you hold (rather than an email address relating to the club) then you will need to consider having consent to continue to contact that individual under PECR. When clubs

do use the school's facilities regularly, you could consider introducing a consent form that clearly states why you intend to hold that data, for how long, and how you intend to use it.

Q - Can admissions data be used to contact families of incoming students, for example to invite them to attend the PTA summer fair? If yes, on what grounds is this acceptable?

A - In most cases, your PTA is a separate entity from the school, therefore you cannot share data with them unless the parent (or future parent) has given specific permission for you to do so. I would recommend asking parents as a part of the enrolment process if they are happy to receive information from the PTA then you could invite them to such events. If sharing parent data with the PTA however, you will need to consider how the PTA is processing this personal data as the school will still have a responsibility to ensure this is being used appropriately.

In many cases, schools will send communications out to parents on the PTA's behalf, so the school doesn't actually share data, however even in this context the school is processing the parents' personal data to promote the PTA activities. As such, you will still need to rely on either consent from the parents to receive this information or to demonstrate that the school has a legitimate interest to promote the summer fair to future parents and this needs to be made clear in your privacy notice. Again, don't forget if relying on e-mail you will need consent under PECR.

Q - Many local estate agents put up boards promoting school summer fairs paying the school/PTA around £25 per board. Parents sign up to agree to take a board. How should this data be collected by the school and how should this be sent on to the estate agent so that they can visit those addresses to put up boards?

A - You would need a data-sharing agreement between the school and the estate agent which includes a clause asking for proof of disposal of the information after a specified period of time – ideally six weeks after the event. Make it clear to parents that their data will be shared with the estate agent and explain the destruction agreement.

Q - How can schools collect Gift Aid information from parents – could this be collected at the start of a new school year when data collection sheets are sent out? As this information will be inputted into the HMRC website, does the school need special wording around the 'sharing' of this data with a third party?

A - Gift Aid information should be collected at the same time as a donation is made and needs to be kept for six full financial years after the financial year in which the donation is made. There are excellent examples of wording available from HMRC which should be followed. As there is a legal basis for retaining this data, there is no need for a data sharing agreement in this case. Please see gov.uk/claim-gift-aid/gift-aid-declarations .

Q - A local primary school organised a junior colour run last autumn with many children from other schools in the area taking part. It was hugely popular and they plan to run it again this autumn. Can they contact those who took part last year, inviting them to join in this year?

A - It depends. You may be able to rely on legitimate interest given you are inviting them to the same event, and contact runners from last year, but you would need to ensure you carry out a

legitimate interest assessment to ensure you have considered their privacy rights and whether your communication is intrusive, and again without consent, you could not contact them by e-mail. Don't forget that you can try and gain new supporters too by publicising the event widely throughout the community. I'd suggest when people sign up to this year's event, you invite them to opt in to receive information for similar activities in the future. If this is an annual event, then you can give them the option of opting in each year and update your database accordingly.

Q - If schools are using an online ticketing platform such as Eventbrite or jumlebee, to sell tickets for a community event (i.e. music festival), are there any issues to consider over using third-party software/payment systems?

A - You will need to consider data sharing agreements and where the data is held (not outside EU otherwise this doesn't comply with GDPR). Most of the big platforms will be aware of the legislation and can guide you. However, you may like to include as part of your privacy policy, that such third-party websites are not covered by your own privacy policy and therefore advise that individuals using these platforms should check that they are happy with the third-party privacy policy before proceeding.

Q - Are there any other relevant issues to consider such as maintaining a database of previous donors or those who have opted out of receiving information?

- You need a list of people who have opted out to prove you are not contacting them
- You need to keep information about donations or financial transactions for a specified period of time - this is legal basis and mandatory
- Consider communication methods - unless people have opted in to receive emails, you cannot contact them that way
- Ensure that you are clear about who the communication has come from. Is it from your PTA, school fund or the school itself? What is the legal basis you have for processing the data? To parents, they will all seem the same, but the reality is that they are separate legal entities and each needs to consider the retention, storage and processing of information.
- Make sure you have a DPO (Data Protection Officer)!

This article has been supplied by IDPE and should only be used as a guide. Every school is different and therefore we recommend that schools seek legal advice or contact the ICO directly for further information.

A summary of GDPR

The General Data Protection Regulation (GDPR) is a new law which will replace the current Data Protection Act. Every organisation that processes personal data will have to comply with the GDPR from 25 May 2018. GDPR focuses on the purpose for processing personal data: organisations must process personal data in a lawful, fair and transparent way, and for specified, explicit and legitimate purposes.

Legal basis for processing personal data

The requirement to have a lawful basis in order to process personal data is not new, however the GDPR places more emphasis on being accountable for and transparent about your lawful basis for

processing. The six lawful bases for processing are broadly similar to the old conditions, however there are some changes for example to the definition of 'consent'.

1 Consent: the individual has given clear consent for you to process their personal data for a specific purpose – under the GDPR, this must be a freely given, specific, informed and unambiguous indication of the individual's wishes (no more pre-ticked boxes)

2 Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract

3 Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations)

4 Vital interests: the processing is necessary to protect someone's life

5 Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law

6 Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Each school will need to review your existing lawful bases for processing personal data, and check that these remain the most appropriate. For further information, visit <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>

Accountability and transparency

The GDPR brings in new accountability and transparency requirements. Your school must clearly demonstrate compliance through documenting your purpose(s) for processing personal data, the appropriate lawful basis (or bases) in your privacy notice(s) and informing individuals about how and why you are processing their personal data, through regularly sharing your privacy notice.

Schools must also consider when and if the purpose for processing personal data changes, for example when a pupil leaves school and the school continue to communicate with them as an alum – has the purpose for processing personal data changed? If so, is this detailed within the school's privacy policy? And has it been shared?

Individual rights

As well as setting out the different bases for processing personal data, the GDPR strengthens the privacy rights of individuals to now include:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing

- The right to data portability
- The right to object (including objecting to direct marketing)
- Rights in relation to automated decision making and profiling

Other key changes under GDPR

- **Contracts** – whenever a data controller uses a data processor (a third party who processes personal data on behalf of the controller) it needs to have a written contract in place.
- **Documentation** – documenting your processing activities, covering areas such as the purpose for processing personal data, data sharing and retention, is a new requirement under the GDPR.
- **DPIAs** – Data Privacy Impact Assessments or DPIAs are the GDPR version of a Privacy Impact Assessment. The GDPR introduces a new obligation to do a DPIA before carrying out processing likely to result in high risk to individuals' interests. If your DPIA identifies a high risk which you cannot mitigate, you must consult with the ICO. You will need to review your existing processing operations and decide whether you need to carry out a DPIA. A DPIA is likely to be necessary if an area of work is new or potentially high risk.
- **DPOs** - The GDPR introduces a duty for you to appoint a Data Protection Officer (DPO) if you are a public authority, or if you carry out certain types of processing activities, or to consider who will take overall responsibility for data protection.
- **Security of personal data** - the GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.
- **International transfer of personal data** - The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.
- **Data breaches** – under the GDPR, there is a duty to inform the ICO within 72 hours (including weekends or out of working hours) if a school has a data breach.