May 2018 sees the introduction of the new General Data Protection Regulations (GDPR). We've spoken to the Fundraising Regulator and the Information Commissioner's Office (ICO) to find out what PTAs need to know

What's changing?

The new regulations mean more stringent rules for how you collect and store supporters' data. This includes everyone from parents and families to businesses and sponsors, and applies to all processing of personal details, meaning it covers fundraising, online campaigns and volunteering. Every time you contact supporters you'll need to explain why you're contacting them and how you will use their data. You need to be compliant with the regulations by 25 May, so familiarise yourselves with them now and start thinking about what measures you need to put in place. GDPR will affect:

- How you collect personal details
- How you contact your supporters
- How you store personal details.

How do PTAs work now?

Within a school context, the school itself is classed as a 'data controller', which means it is the party that decides how personal data is processed. The PTA sits under that as a 'data processor', where they process data on behalf of the school (or data controller). The act of processing data covers collecting and recording information as well as holding and storing it.

A quick survey of PTAs found that the most popular form of communication is social media, with a huge 89% of people using it to contact their supporters. 79% of PTAs use letters in book bags, and 78% have the school send communications on their behalf.

PTAs are fluid organisations that can change dramatically from year to year, meaning there isn't always one person overseeing areas such as data protection. While everyone's main focus is organising and running fundraising activities, data protection can be easily overlooked. Risks may not always be obvious, but 22% of the PTAs we surveyed send emails from private email accounts, and many also have parents' data stored on personal computers with no measures in place to ensure this is deleted when they leave the PTA. So what needs to change?

When do GDPR rules apply?

The first important thing to note is that the new GDPR rules only apply when you use personal data. So you can send indirect communications, – a flyer in book bags, for example, promoting a PTA event. This isn't using personal data because you aren't including any information that identifies a specific individual. Even if parents opt out of receiving communications from the PTA, a flyer in a book bag is still permissible because it isn't specifically targeted.

However, if you use supporters' contact details to keep in touch with them about your PTA, that is direct marketing and the new rules will apply. Direct marketing is defined in the Data Protection Act as: 'the communication (by whatever means) of an advertising or marketing material which is directed at particular individuals'. In these circumstances, you will need to establish a legal way to use supporters' data. For most PTAs, the two most applicable ways to do this are 'consent' and 'legitimate interest'. You need to choose the most appropriate way based on what you want to do.

Obtaining consent

A significant change under GDPR is the need for your supporters to actively consent to receiving communications. This means that individuals need to agree to being contacted by the PTA. This could be by simply ticking an opt-in box on a form. The individual must fully understand that they are giving consent for you to contact them, as well as what they're agreeing to be contacted about, why their personal information is being collected, what you will do with their information, and to which form of communication it applies, i.e. email and/or SMS.

Obtaining initial consent may be tricky, as you cannot send texts or emails without prior permission, including messages asking for permission! The safest way to get consent is through paper form, which can be distributed without using personal data through book bags (see 'when do GDPR rules apply?') or by mail (see 'legitimate interest' overleaf). This form should tell your supporters what kind of communications you would like to send and ask supporters to tick an opt-in box confirming that they are happy to be contacted. You should include a tick box for each channel (e.g. emails, texts, post) and they should tick all that they are happy

with. Other acceptable forms of consent include:

- A tick box or yes/no option on a donation form.
- An individual supplying their contact details on a form or online, where it has been made clear they are doing so in order to receive direct marketing from the PTA.
- Orally or by a clear action, e.g. an individual handing over a business card and making it plain they want to hear more from you.

Whatever the case, the opt-in needs to be separate from any other action, and individuals need to have consciously given consent based on explicit information. Silence or pre-ticked boxes are not valid, nor is the assumption that people are happy to be contacted unless they have opted out.

Withdrawing consent

People's preferences change over time, so it needs to be easy for your supporters to withdraw their consent or change communication choices whenever they wish. Let your supporters know how they can do this – for example, they may need to email a certain phrase to your PTA's email address. Be realistic about the amount of paperwork you can cope with versus compliance with GDPR. As schools usually send out data information sheets once per year, it is perfectly viable that your PTA does the same. Bear in mind that you will also need to manage and maintain a 'suppressed contacts' list of people who have opted out of receiving PTA communications.

Sign up to receive PTA+ newsletters and we'll let you know as further GDPR guidance becomes available. Go to pta.co.uk/sign-up.

Third parties

You may find that it's sometimes necessary to input personal data into a third-party website, e.g. loading email addresses into Eventbrite. You cannot disclose data to a third party without consent, so you can only do this if the individuals were aware – at the point of collection – that their data would be used in this way.

Contacting supporters – legitimate interest

Aside from obtaining consent, another way you can legally send out direct marketing is via 'legitimate interest'. This only applies to an addressed letter (for example, to 'Mrs Brown' or 'The parents of Jane Smith') or a phone call. This method relies on you being able to justify that the PTA has an evident legitimate interest in sending the communication, and that the individual you are contacting has a legitimate interest in hearing from the PTA.

This requires you to balance your own interests against the rights and interests of the individual – something that is particularly significant when it comes to children, as they are identified as a vulnerable group by GDPR. In cases where you plan to contact children directly using their personal data, it is likely to be much more difficult to prove a legitimate interest, as they are less likely to be in a position to object to the communication than an adult.

Legitimate interest should be considered on a case-by-case basis, taking into account the reasonable expectations of the recipient. In many cases, the fact that someone is a parent at the school may be justification enough. But if the individual would not reasonably expect you to use their personal details to contact them (for example, where they have previously objected to contact or where there is no prior relationship), this would not be legitimate interest and you must not contact them. The key question to ask is, 'if I were in their shoes, would I be surprised to receive this?'

It's vital that you document your justification for using legitimate interest. This will act as protection should you be challenged by the individual or regulator. You would need to show clearly documented evidence that the individual's rights and reasonable expectations were balanced against your legitimate interest before the decision to send the communication was made.

When sending communications via legitimate interest you must give individuals the chance to opt in to receive future direct marketing.

Should we rely on consent or legitimate interest?

Although GDPR doesn't require an opt-in for all communications, the ICO and Fundraising Regulator agree that 'consent to contact' is the most reliable basis for direct marketing. In the case of PTAs, however, it could be argued that as all parents at the school have a child who will benefit from the work of the PTA, all parents could be contacted through legitimate interest (as long as they haven't opted out). It may, therefore, be practical to use a 'legitimate interest' enquiry to seek consent from individuals for them to receive communications via electronic channels and rely on flyers in book bags for general marketing purposes.

Electronic communication

Under the Privacy and Electronic Communications Regulations (PECR) – extra rules that sit alongside GDPR – further criteria applies to communication channels:

Digital messaging (text or email): You can only contact someone via these if they have given clear consent. This includes a message asking if an individual is happy to keep hearing from you. If you do not know if an individual has consented to being contacted via digital messaging, you must not contact them in this way. (Some providers have compliant systems – see Classlist information above).

Telephone: You may contact someone via telephone if it is a live person-to-person call and the individual has not opted out of telephone marketing. As PTAs don't have access to the Telephone Preference Service, contacting people via telephone can be risky and it is safer to use other forms of contact. Contacting businesses – with requests for sponsorship or donations – would be fine, as they are unlikely to have signed up to the Telephone Preference Service (TPS).

Facebook: If a supporter has joined your PTA Facebook group, then you can message an individual, as the act of joining shows that they expect to hear from you. It isn't acceptable to message individuals' personal profiles when they have shown no interest in the PTA. Messages are unsolicited if they haven't been requested, but even though an opt-in doesn't make a message solicited, it does make it more likely that your marketing is compliant with PECR. Unsolicited or not, you must always say who you are, include appropriate contact details and ideally give people the option to actively opt-in to receive further communications.

As these rules may change the methods you currently use, it's crucial to consider how you will seek consent from your supporters, how you might need to alter your communications, and how you manage any data you hold, including suppressed lists (see overleaf).

Social media

89% of PTAs use social media to communicate with parents. While this is a useful tool, it can pose a variety of data protection and security issues. You need to be fully aware of your page's privacy settings and who can access the information you post there. For example, some PTAs post a phone number through which parents can contact the PTA, but if your privacy settings are not restricted then anyone who visits your page could see it. Think about how you've authenticated members of social media groups: are they real parents – or even real people?

Public social media pages can be a brilliant way of promoting your

How can you work with the school to ensure that you're compliant?

Schools have received guidance and training on GDPR, and as the holder of highly sensitive data have to be on top of compliance. Make use of this knowledge if you are unsure of what measures to put in place. They should also be able to give you specific advice – with opt-in wording on letters, for example.

Alternatively, merging communications with the school is a good way to ensure you are supported. Having the school provide an additional option to accept communications from the PTA when gathering their own opt-ins is a practical way to gather initial consent. Alternatively, if the school were to include a PTA section within their regular newsletters, this would be covered by the consent given to the school as it is their communication.

If you're unsure about storing data for yourselves, see if it's possible for the school to store data for you through their system.

The Classlist solution

Relying on spreadsheets or asking your school office to forward PTA messages aren't ideal solutions when it comes to navigating the data protection minefield. That's where a specialist communication tool such as Classlist fits in.

Classlist is a free app that has been specifically designed to give PTAs a quick and legal way of creating a parent database, where parents themselves upload and share their own data. Classlist has worked with top lawyers to develop a neat and practical solution that actually takes advantage of some of the new GDPR provisions. Using Classlist means you can ask you school, entirely lawfully, to help you validate and update information. The app enables the PTA to build a secure online parent community where parents themselves choose what contact details to share. You can create and manage events, send and monitor announcements and put items up for sale. Once your PTA sets up a Classlist account, invite those parents you are already in contact with by email – they can also join directly through the website. Those who don't wish to join will continue to receive PTA communications through Classlist's email system, which is entirely compliant with the new legislation. The system is far more secure than spreadsheets or social media and solves the problem of class reps using different methods to reach different parents, or having to wait for the school office to send important messages out.

Best of all, Classlist is entirely free – indeed, it's funded by local advertising, and PTAs who find local sponsors keep half of the revenue, so it could even generate an income too!

From the school's perspective this solves numerous headaches – it frees up time from the school office, and they can be confident that parent data is managed by the PTA in a secure, private and legally compliant manner. The school can also help by providing you with checklists of parents and parent emails to help validate new joiners, and help you update class lists at the end of term or school year. One of the added benefits of Classlist is that it includes the ability to send messages to groups, making it easy to let parents of Year 6 children know about an end-of-year party, or set up a group to manage summer fair volunteers.

As parents manage their own Classlist account, they can opt into different groups or message preferences, meaning the PTA doesn't need to worry about this.

Setting up Classlist is straightforward. You alert parents a couple of weeks in advance through your website or newsletter, then issue invitations. Having your Headteacher publicise the rollout really helps bring parents on board quickly. Classlist provides all the draft letters and notices you need to launch whilst complying with the new GDPR regulations.

For more information and to sign up, visit classlist.com.

IMAGE: ELENABS/THINKSTOCK.CO.UK

fundraising to a wider audience, so don't feel that you can't have a page. It may be safer, however, to have a secure, closed group for your committee and/or parents, as well as a page where only general information is posted.

The changeable nature of a PTA committee means that you may have a dedicated moderator one year, and then the page, or group, may go unmanaged the next. Try to overcome this by creating a dedicated social media officer role.

Storing data – databases

Under GDPR it's important to keep clear records of what a person has consented to and when they did so. This means procedures for using and protecting personal data need to be documented. If you are unable to show that you have ongoing consent and when you got it (or up-to-date information to justify legitimate interest) then you cannot use personal data for direct marketing. The best way to do this is to set up a secure and well-maintained database of all personal data you possess.

Collins Dictionary describes a database as 'a collection of data that is stored in a computer and that can be easily used and added to'. This covers spreadsheets, Google Docs and Word documents – but lists on bits of paper still count! Of the 80% of schools who handle their own data, 56% use an Excel spreadsheet and 36% use Google Docs to keep information safe.

To comply with GDPR you should be able to demonstrate that:

- All personal data is stored securely in one place.
- Data is regularly reviewed and updated.
- Your database is password protected and the password is not handed out too freely.
- You keep track of who has access to the data and remove access/update the password once members leave the committee.
- Have a written policy and keep a record of how you handle data.

If you already have a database, start as you mean to go on by updating it as best you can. If you have individuals on your database where you don't know when you last interacted with them or whether they gave consent, then you cannot safely contact them and need permission before doing so. You also need to keep the data of any business or sponsorship associates safe – all data needs to be treated and protected equally.

Finding out who does and doesn't want to be contacted is one thing, but keeping this information safe within itself is also crucial. The easiest way to do this is by splitting your database between those who have opted in to receive PTA communications and those who haven't, as well as those who have actively said they do not want to be contacted. Keeping all data in one place means it can be easily passed over when the committee changes, and there's no risk of the new committee emailing those who have opted out.

Keeping data contained is a practice that should be extended to emails too. It's hard to keep track of emails sent from numerous personal accounts – one PTA email account that various people can access means everything is in the same place and there are no concerns over personal data on private accounts.

What else do you need to know?

Data breach: All organisations have a duty to report certain types of data breach to a relevant supervisory authority. A data breach is defined as, 'a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. This means that a breach is more than just losing personal data. You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals – this would need to be assessed on a case-by-case basis. A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. For more information, visit **ico.org.uk**. Check that your PTA insurance policy specifically covers data protection and the cost of seeking legal advice in the event of a data breach.

Deletion policy: There is no stipulation for the length of time data is kept and some personal data will need to be retained for longer in certain cases. How long you retain different categories of personal data should be based on individual needs. A judgement must be made about: the current and future value of the information; the costs, risks and liabilities associated with retaining the information; and the ease or difficulty of making sure it remains accurate and up-to-date. For example, one to two years would seem reasonable for parent data (though if you are asking parents for consent annually, it might be easier to start your parent contact database afresh each year).

That said, you may wish to securely archive the previous year's data in case of repeated activity, such as a Christmas pudding scheme in which parents have previously participated. Contact details for businesses who have provided sponsorship or donated raffle prizes in the past could reasonably be kept for longer. Make sure you agree a process and, if you can, attribute responsibility for data management to someone on your committee.

For more information

If in doubt, seek expert advice. Find more guidance from the following organisations:

- Fundraising Regulator: **https://goo.gl/FBTcdp**
- ICO: **https://goo.gl/nVc4kP**

ICO has a helpline for smaller organisations preparing for GDPR: 0303 123 1113.