Parentkind
Bringing together home & school

GDPR guidance for PTAs

UK Information Commissioner Elizabeth Denham said:

“The new data protection laws apply to all organisations – even small charities such as Parent Teacher Associations. **Parentkind have prepared some excellent, easy to understand guidance which should prove to be extremely useful for members**. People are starting to judge organisations by how they look after their data. That is why the new laws are a great opportunity for organisations to enhance their reputation and trust with those they work with.”

The guidance set out below is based on our organisational interpretation of the guidance issued by the Information Commissioners Office (ICO) on compliance with data protection law in the UK.

This is not legal advice, this is our best interpretation of the current guidance that has been provided by a range of sources none of which refers to the specific circumstance of PTAs and there is no case law in this field. We will endeavour to update this guidance regularly with any relevant changes.

The General Data Protection Regulation became law in the UK on 25 May 2018. The majority of underlying principles have not changing, but there are big changes to the accountability and transparency required by organisations. And they'll have an effect on all organisations that use personal information, including PTAs.

We are urging all committee members to read this information, and assign one member of the committee to lead on this for your PTA, encouraging them to become sufficiently knowledgeable about how it affects your PTA.

For us as individuals, the GDPR and the new ePrivacy Regulation are a good thing. It will mean organisations and companies have to treat our data more carefully, and take more care about making sure communications from them are wanted. It should reduce spam emails and calls, and make our children and their data safer too.

As members of organisations, the GDPR will mean a few challenges and extra work. But with a bit of common sense there's nothing that will be too hard for most PTAs. This, also, represents a great opportunity to re-engage school staff and parents in what you do. This infosheet sets out what the regulations are and provides guidance on the standards that need to be met in order to comply.

How is the law changing?

Data protection law is quite complicated, and involves a lot of jargon and acronyms. You'll find definitions and explanations of the most common terms in the GDPR Glossary at the bottom of the page - look out for the links.

The law in place now

Currently there are two main data protection laws covering the work done by PTAs:

1. The Data Protection Act 1998 (DPA 1998). This is being replaced because it's seen as out of date for today's very different digital world.

2. The Privacy and Electronic Communications Regulations (PECR) which set out what organisations can do when communicating electronically. These communications cover marketing calls, emails, texts and faxes, as well as "cookies", which are small pieces of code used to track visitors to a website. (Those pop-ups found on most websites, asking you to agree to cookies or go away, are due to these regulations.)

How will these change?

1. The DPA 1998 is going, and will be replaced by the Data Protection Act 2018 (DPA 2018). The **General Data Protection Regulation (GDPR)** will be adopted on 25 May 2018, because the UK is in the EU. The date is fixed and this will definitely happen. The Data Protection Act 2018 will then maintain the requirements of the GDPR once we leave the EU.

2. The PECR is going, and will be replaced by the **"ePrivacy Regulation"**. We don't yet have a date for when this will happen.

Our message to PTAs is that they should prepare for the GDPR, but just keep watching out for updates on the eprivacy regulations for now. We'll also be sure to update this information for you, when more information on this is available.

What do these regulations cover?

The GDPR covers **the** processing of personal data, also referred to as personal information in this guidance, by any organisation (including PTAs) wherever that takes place. The key point is that it doesn't matter if you're processing the data in a committee member's home, if it is on behalf of the PTA, it is covered by GDPR. Personal data means **anything** that can identify an individual, including:

- Names
- Email addresses
- Home addresses
- Phone numbers
- Medical history
- Dietary requirements
- Age and more.

If a piece of information tells you anything at all about a living person, no matter how small or trivial, assume that it's covered. It doesn't matter what format the data is in - digital or hard copy - it is still likely to be covered by GDPR regulation.

Processing can mean doing something with the data, such as using it to send an email, or

sharing a list of names with your Treasurer so they can match them up with event payments. More surprisingly, the **storage** of data is also included as "processing". For example, a list of names and telephone numbers sorted alphabetically by surname in the PTA filing drawer no-one has looked at for three years is also covered.

One thing to note; it is only when what you do involves the **processing of personal information** that is it covered by this regulation. If, for example, you produce a general newsletter, and you ask the school to put a copy in every book bag, because they are not addressed to anyone, and you have used no personal data such as email or name and address to send them, then **this is not** covered. On the other hand, if the newsletter goes by email, all the email addresses you send it to are personal information of the recipient, therefore it is covered.

Does it affect all organisations? Even small PTAs?

Yes. Parentkind has looked into this in detail, and consulted experts and the relevant regulatory body, the Information Commissioner's Office. There are no exemptions.

PTAs are small independent charities (regardless of size, registration with the Charity Commission or having a constitution), that make their own decisions about what personal information to collect, how to store it, who can access it and how to use it. That means they count as a "Data Controller" - an organisation responsible for processing data - so have to obey the GDPR.

Preparing for the GDPR: Do you have the right to keep your data?

The GDPR has a limited set of reasons why an organisation can collect, keep and use personal information. These are covered below. But before considering the legal side of things, ask yourself what *your* reasons for processing the data are.

Challenge your association to justify exactly **why** it needs the information it collects and holds. Sometimes it will be easy; you need your committee members' phone numbers to arrange meetings, for instance. Sometimes less so; what use is a 2015 year 6 disco attendance list now? Write down all of the information you have and all you need in a list.

This list - termed an information register - of everything you hold and your rationale for holding it will be incredibly useful in all your future efforts to make sure you're complying with the GDPR.

If you conclude that you don't need a bit of data, just get rid of it, securely (see below). Hoarding personal information, keeping it "just in case", can't be justified and will likely leave you in a difficult legal position.

What's your Lawful Basis for Processing?

In the GDPR there are **six** reasons, or "Lawful Bases", why you are allowed to collect, keep and use personal information. These are quite detailed and we explain the relevance below.

1. Consent. This is an important one, which may be the most relevant to PTAs.

To rely on consent as a reason, the person whose data you have, or their parent/guardian if they are a child, must have:

1. had it made **completely** clear to them what they were consenting to have their data used for, and then you must stick to those reasons. If you ask for consent to update people about the Roller Disco, you can only communicate to them about that one event. We would therefore recommend that you ask people for consent to communicate with them about **all** your PTA events.
2. clearly told you that they agree to you using their personal information by doing something **active** to tell you, such as ticking a box, putting their name down, or replying positively to an email. Simply leaving things as they are e.g. not unticking an already ticked box, or crossing out a line consenting to use of data, will not do.

You'll need to keep a record of the consent to show it comes up to these standards:

- You **must** use consent for all activities defined by data protection law as "marketing" when you are sending communications **electronically**. A far broader range of activities is considered marketing by the PECR than PTAs may expect. They include, of course, asking people to donate or buy merchandise, but also asking them to come to or volunteer at events, sign up to newsletters, enter competitions, or even just tell them about PTA successes. Phoning people, using email, text or social media is considered electronic communications
- Sending home flyers in book bags, or through doors, which aren't directly addressed to people, is not usually considered direct marketing and therefore the rules won't apply. This is because it is information in hard copy which is not being sent directly to an individual using personal data. You may choose to get consent for these activities as the right option, but the law doesn't require you to.
- If you have existing personal information for which you have previously obtained consent to use, you need to make sure that the consent you have reaches the new standards given above. Otherwise, you will have to ask for consent again, before 25 May. There is very little wiggle room here. All consent will have to come up to these standards or the data can't be used.
- There is some personal information which you will need to hold because of other laws (see below.) Examples might be financial transactions for tax law reasons, or committee members' details you have to keep for charity law. Where this is the case, someone giving or withdrawing their consent wouldn't make any difference to whether you carried on holding this information, it is therefore not appropriate to ask for consent.

2. Contracts. If you need someone's personal information to perform a contract with that person, you can process it.

For example, if you have booked a bouncy castle for your event, you can keep personal information of the supplier, in order to fulfil your part of the contract and pay for it. It gets slightly

more complicated when the PTA is a middleman. For example - you have set up an online shop with a hoodie supply company, and whilst the parents are in the end paying the hoodie company direct, you are handling their personal information to make sure the orders go correctly. Here you can hold and process this information, but only for as long as is necessary, and this would almost certainly be under the legitimate interests basis, see point 6 below.

3. Legal obligation. This comes into play if the law requires you to keep, process or pass on information about someone to another organisation. For example, the chair of a PTA which is a registered charity will have a legal obligation to send your committee members' details to the Charity Commission.

4. Vital interests. This basically means that you need to hold and use personal information to protect someone from serious injury or death. Not many reasons spring to mind as to why a PTA might need this although you should also read the section on Special Category Personal Data.

5. Public task. PTAs can ignore this one as it applies to organisations that carry out a public task, which is required by law. One example would be your local authority, or water company.

6. Legitimate interests. This is the most vaguely defined and confusing of the possible reasons to use data, however it is also the most flexible!

Put simply, it boils down to whether your PTA, the school, the parents or the children have a justifiable reason for you to hold and use the personal information. Put yourself in the shoes of a parent at the school whose data (or whose children's data) you are using, and ask yourself, “if I was the parent, would I expect the information to be processed in this way?" If you're not convinced the answer would be "yes," then don't rely on this reason.

In order to use legitimate interest as your reason for data processing, you'll need to be able to prove that you have considered the fundamental rights and freedoms, including the rights to privacy, of the person the data is about.

Deciding when you can use legitimate interest can be tricky:

- You **may** be able to use legitimate interest as a basis for communicating with your members on things that aren't marketing, such as AGM details, updates on financial performance, information on new committee members etc, by electronic means.
- You **may** be able to use legitimate interest as a basis for sending information **by post**, asking parents to come to events, enter competitions, volunteer, sign up to newsletters, buy merchandise, and to generally update them on what your PTA is doing, for example.
- You **should not** use legitimate interest as a basis for any activities considered by law as "electronic marketing". Remember, this has a much broader definition than you might expect, including activities such as asking parents or pupils to come to events, enter competitions, volunteer, buy merchandise, sign up to newsletters or social media groups, or even to send a newsletter or update on the progress of a fundraising project.

You can find further information about using legitimate interests in the glossary.

How should you collect and obtain personal information?

Getting things right when you collect data in the first place is key to keeping on the right side of data protection law.

What should you collect?

The first rule of the GDPR is don't collect anything you don't need. So really think things through before you jot down a single name. If you are only ever planning to email parents, why do you need their home address? This is why it's so important to write down what you've got and why - it will help you spot what you can stop collecting or get rid of.

Collecting data you don't need is not only pointless, but burdens you with potential legal liabilities. If someone steals your treasurer's computer and so accesses and uses personal details the treasurer needed and used, that's one thing. The blame and any penalties will likely largely fall on the criminal (so long as you kept the details reasonably secure - see later). If the computer is full of personal information that you should no longer have, however, the liability for its loss is, in part, the treasurer's, and if they have not been advised correctly, the PTA's.

Never collect personal information if you don't need it, or just in case you might need it in the future. You **must** collect information only for a specific purpose, one which you're clear on at the time the information is obtained; not thought up later.

How should you collect it?

There are different things to be aware of depending on how information you hold and use reaches you.

Information coming directly from parents?

If you need consent from parents to use their information, be specific and smart about what you're asking for to make sure it encompasses everything you may need consent for over the year. (Remember that you may not need consent for all your processing as there may be another legal basis that applies.) Getting this in writing is important so you have a record, should you ever need to prove you did things properly. When we say 'in writing': emails, web forms etc. are included and are OK, as long as you keep a record of what you asked, how they consented and when. Keeping originals, where possible, is recommended.

You need to make the following things clear when you ask them for consent to use their information:

- Exactly what you are asking them to consent to; spelt out as clearly as possible
- That they can withdraw consent at any time, and how they can do this (it should be just as easy to do as it was to sign up).

At this stage you also need to provide information on what you're going to do with their data. This is called your privacy statement - you can put key points only on a paper form, (and refer to a full

version online) if you need to. This is called a **layered approach.**

The same rules apply to parents and to pupils, except that the person with parental responsibility has to give consent for a child.

If you are not relying on consent but on one of the other legal bases, explained above, you must make this clear on your privacy statement and make it clear they have the right to object to your legitimate interest or withdraw their consent.

Information sent to you by the school

If you need consent from parents to use their or their child's data, make sure the school has collected this. PTAs are independent organisations, separate from the schools they support, so the school should ask parents' permission to pass information to you. In law, it's their responsibility if they don't, but it's best to get this right for the sake of keeping a good relationship and avoiding problems. You then have one month to provide information to the parents/children about how their personal information will be processed.

It's wise to have a written agreement between your PTA and the school outlining what information is being passed between them. This is called an 'information sharing agreement'. If you're not sure about, or think something is wrong in the agreement, ask the school for clarification. Once you've agreed it with the school, make sure all your members stick to the terms of the agreement. If the school is going to collect their parents' consent for communications, there is no reason why they cannot ask for consent for the PTA at the same time providing they supply your privacy statement information. As long as the question(s) is/are clear, this could save effort. It is worth talking to your school early about this.

If you are not relying on consent but on one of the other legal bases explained above, you must make this clear on your privacy statement; reference this each time someone whose data you are using contacts you, and make it clear they have the right to object if you are using the legitimate interest basis. The right to object is one of the fundamental rights that people have if you are processing their personal information, and once you receive one of these objections (if you ever do) you must investigate, document the conclusions, and tell them in writing – even if you don't agree.

Let's say there is a particularly troublesome parent at your school who has come to your events in the past and verbally abused your volunteers. You have decided to retain his information to prevent his entry under your 'legitimate interest' in carrying out a safe event. He objects to you processing his information for these purposes. You must then double-check the reasoning and if you are confident that your interest overwhelms his individual rights to privacy you can continue to process this data. You must inform him of your conclusions but the point here is, just because he has objected, it does not mean you absolutely 100% cannot process that data any more.

People have a number of other rights if you are processing their personal information and you can find further information about these in the glossary.

Information sent by other people, including parents

If you are passed personal information by third parties, you can use it only after you have informed the data subject what information you have, where it came from and what you will use it for. If you need their consent to process their information, you should not use their details until you have their consent, and if they don't give it, you can't use the information and should get rid of it. Receiving an email from a third party is a good example of some personal information you would almost certainly use for marketing and therefore need consent for.

What you must do, in all cases where you get personal information indirectly, is let the people it concerns know, within one month. That means writing to them to let them know that:

- You have their information
- Exactly what information you have
- Where you got it from
- What you will use it for
- That they have the right to withdraw consent or object to your legitimate interest or other reason for holding the information
- You must also include your privacy statement or a link to it.

Keeping all of the information you have safe

There's not much point in doing everything right on collecting information if you don't keep it safe while you're holding it - but the good news is that having decent information security isn't rocket science.

There are two sides to keeping information safe:

1. The systems you use to store and share information - whether electronic or physical

If you store information electronically, you can make this more secure by:

- Password protecting computers that have the information on them, such as your home computer
- Password protecting files and folders that contain PTA information, so that only you or other permitted PTA members can access them, even on shared computers
- Having up-to-date antivirus software that protects your PC and email account
- Using secure file sharing systems rather than emailing copies of data around your committee.

If you transfer information electronically, such as sending details of event volunteers or attendees to PTA committee members organising them, you can do so more securely by encrypting your emails. This can cost money though (and be quite technical), however, this is required by the regulator for sensitive personal information such as medical conditions.

We would recommend removing the need to email personal information across your committee by using one central file store, which is secured by a password and can be accessed

online. Secure online file sharing sites can help you here, but do read the small print, as your PTA is responsible for making sure you choose a system which states it complies with the GDPR, and describes how they meet the requirements of the legislation. The law prevents you from using systems which transfer or store your details outside the European Economic Area, unless the system has appropriate safeguards in place. One example is the Privacy Shield Scheme. Further information about the safeguards required is available from the ICO's website.

Make sure you can easily add **and remove** access to central file stores for incoming and outgoing PTA volunteers and committee members.

Your PTA may also use social media to share information more widely and promote the good work you are doing; there are a number of apps that will allow you to do this easily and very effectively. If the information you are posting as a PTA allows people to be identified, then it must comply with data protection laws. This may include photos, a blog about activities people have been running and those who attended, or a video clip. **Posting information on a public forum is considered a processing activity that is covered by data protection law. Remember:** If you are processing personal information, then you must have a lawful basis for doing so. These were covered earlier in the guidance. For most posts, you are likely to need consent for publishing personal information and this must also comply with the rules around consent.

You should also control administrator access and ensure those that can post on behalf of your PTA have an understanding of what should and should not be published.

If you are clear on the Facebook page, about what you will communicate to people about when they've joined the group, we feel you can take their act of joining the group as consent. Data protection rules do not usually apply to people choosing to post information on social media about themselves or their children, although you should be very careful about reusing any personal information posted on your PTA forums by others without consent. It would also be good practice to regularly remind your members and those in your groups that not everyone is happy for their personal information to be made publicly available. It is considerate to ask for people's permission before posting personal information about them or their children. Sometimes it can be difficult to decide when a post falls within data protection rules, and there is a link to further advice in the glossary.

If you store information physically, you can secure it by:

- Keeping it in a locked filing cabinet or cupboard
- Making sure only people who need access have it.

2. Your information security behaviour

Make sure housekeeping is high on the agenda. Don't leave personal information around the place, such as leaving your list of volunteer contact details in view on the front desk at the summer fair, and destroy copies of information as soon as you stop needing them.

Our other suggestions are:

- Don't give everyone access to everything. Only give those who need it access and only give them access to what they need. Blanket access for all committee members is not good enough or required
- Don't use USB sticks unless they are encrypted and password protected
- Don't hoard any information 'just in case' it comes in handy
- Have a policy and procedure for information to be given back or deleted by outgoing committee members
- Don't duplicate information unnecessarily.

Marketing your events and activities

The data protection laws have a very broad definition of what is marketing. It includes all PTA fundraising activities, including encouraging parents or the community to attend events, volunteer at events, sponsor children etc. It also specifically includes non-profit groups updating members on successes or championing their aims and ideals.

Direct Digital Messages from PTA to Parent

If you send marketing materials by email, text, phone, social media, WhatsApp or fax, or any other digital means, you must have explicit consent from parents meeting the standards highlighted above.

Digital Messages Sent by the School on behalf of the PTA

We have checked with the ICO, and if a school sends messages about PTA events on your behalf, for example, through Parentmail, or the schools email lists, they must have specific consent to communicate with parents about PTA matters. If the school doesn’t have this already, they will have to ask parents to opt in to receiving marketing messages from the PTA, meeting the consent standards above. In our opinion, the school can ask for this consent at the same time that it asks for consent for its own means, so it doesn’t have to be an additional burden. Our advice is to work with your school as early as possible to ensure this is covered, by approaching them to talk about meeting this challenge together.

Note, this guidance does not apply to non-digital marketing, you may be able to rely on a different legal basis for that marketing.

Destroying personal information

Data protection law requires you to only keep personal information for as long as it is required for the purpose it was collected in the first place. To make sure you're doing this, you need to:

- Know what you've got
- Have agreed timelines for deleting what you've got.

The timescales you need to keep information for can vary. For example:

You have collected information to run a specific event in collaboration with the school. The

information includes a list of children attending, along with the name and emergency contact details for one of their parents for each of them. There is a charge for the event, and so you also keep a list of which parents have paid.

Most of the information relating to this event should be securely destroyed once it finishes, as there's no reason to keep holding it. But you may need to keep a limited amount of information to do with payments for the event to comply with tax and financial reporting laws, usually for six years from the end of the current tax year.

To make sure you comply with the law, PTAs will need to:

- Have a PTA policy on how long you keep each piece of personal information. It would be best practice to add this to your information register (see glossary).
- Have a policy to regularly review personal information you are holding, for example, contact lists, to make sure it is accurate and up to date.
- Make sure each person who has personal information is able to securely destroy that information.
- Regularly remind people receiving personal information about how long it should be kept.
- Don't use a blanket policy on how long things should be kept for, such as "keep everything for one year". Make a decision on how long to keep each type of information depending upon the reason that you are keeping it.
- Don't assume people will remember to destroy personal information or that it has been destroyed. Make sure you have appropriate procedures to regularly check that people have only retained information that they should continue to hold.

When you destroy data, make sure you do it so that it can't be restored and end up in the wrong hands. Shred paper documents containing personal information. Empty the recycle bin after deleting files on a computer. Format USB drives rather than just deleting files off them.

Is there anything else our PTA should know?

There are a few categories of data for which the GDPR has special rules, which may affect PTAs.

Special Categories of Personal Data

This is a new term in the GDPR for personal information on some subjects which has an extra level of sensitivity attached. It covers race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life and sexual orientation. The current name for this information is sensitive personal data.

If you want to use personal information which is in one of these categories, then your PTA is likely to have only two possible legal reasons for doing so open to you:

- Express, explicit consent from the person the data is about, or their parent or guardian (if a child)

- To protect the vital interests of the person the data is about. As we stated earlier, this has to be quite literally a life and death situation.

In reality, the only sort of special category data that may be needed by PTAs is health data, for example about allergies or medical conditions affecting children or volunteers that those running an event might be required to know.

For example, if your PTA was organising a disco where there was food, and had been passed information on allergies affecting some of the children by the school, you would obviously first attempt to gain parental consent to pass this information to organisers. But if you weren't able to do that, you could still lawfully pass this information to those running the event as that's necessary to protect the "vital interests" of the children.

You should note that this wouldn't allow your PTA to continue to hold the information, it would need to be destroyed after the event. It's very unlikely that storing information would ever be required to protect someone's "vital interests", so you should assume you will need consent if you want to continue to hold these details.

Special rules for children

The GDPR states that children under a certain age cannot give consent themselves to use online services, e.g. Facebook, Mathletics or Minecraft, and a person with parental responsibility needs to give consent.

The DPA 18 has some further guidance on age, lowering the age of consent for information society services to 13. In practice, we doubt there will be any considerable change to the current interpretation, which is whatever age they are deemed to understand the consequences of their actions. Most young people would have some capacity for understanding the implications of signing up to receive e-mails. If there were contractual obligations this would have an effect on complexity, and might be differently interpreted.

What happens if we don't comply with the GDPR?

Theoretically, the maximum fine is €20M or 4% of turnover, whichever is greater, which is obviously a very large deterrent, and has had a lot of air time in the media.

These laws will be enforced in the UK by the Information Commissioners Office (the ICO). The ICO does two things, it is a proactive body that issues compliance guidance it expects us all to follow. It is also a reactive body that responds to complaints about how personal information is being processed, or investigates when organisations refer themselves (as the law requires if they suffer a serious data breach).

It is likely that the biggest offenders will be prioritised and investigated first. If you do not comply with the laws and the ICO become involved in auditing or investigating your PTA, depending on their conclusions they may penalise you. Currently, if organisations consent to audits, they are not usually penalised if they implement recommendations.

A new risk is that affected people can bring their own actions, as the GDPR introduces

compensation for non-material damage, such as distress. Your reputation as an organisation may also be damaged. Often it is the reputational damage that costs organisations more than the actual fine.

If you are unsure about specific compliance circumstances, contact our support line, or ask the ICO small organisations helpline.

The GDPR Glossary

Legal Terms

Some of the words we have used in this guidance have a specific meaning when we use them to talk about the requirements of data protection laws. These are:

Data controller – this is the current term under the DPA 1998, which will become **controller** under the GDPR. A controller "…determines the purposes and means of the processing of personal data".

This will be your PTA. You decide what information you need, why you need it and how it is processed.

Data processor – this is the current term under the DPA 1998, which will become **processor** under the GDPR. A processor "…processes personal data on behalf of the controller".

This does not include those who are members of your PTA although This is likely to include any organisations providing products and services you are using to help you manage your PTA information. This could be the school sending something out for example via their Parentmail. Further information and guidance is available here.

Direct marketing means

"the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals".

Electronic direct marketing (for example, information sent to a person by e-mail) will need to comply with the PECR as well as the GDPR and you will need to use consent as the lawful basis to process personal information. Where direct marketing is not electronic, for example you send information by post, you may be able to use legitimate interests as the lawful basis (see the balancing test) although don't forget that you should still offer people an option of opting out. You must also comply with any request to remove them from your marketing list if they don't wish to receive your information.

Personal data means

" any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is anybody who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental,

economic, cultural or social identity of that natural person."

It is important to understand that information is considered personal if anyone can identify a person from the information, and not just when someone in your PTA is able to identify them. For example, an image that clearly shows a person's face will be personal data, even if you don't know who they are.

Processing means

"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

Almost anything you want to do with personal information, including storage, falls within data protection rules.

Other Terms

We have also used some terms that refer to very specific parts of the different laws that apply. These are explained below, together with links to further information that is available. We haven't covered these in much detail within this guidance. However it is important that those responsible for looking after personal information within your PTA know that there may be additional requirements for using personal information for purposes not covered in this guidance:

Balancing test

Before deciding to use legitimate interests as a lawful basis for processing, it is important to assess whether it is suitable in the context in which you wish to use it. There is a three-part test:

1. The purpose test – are you pursuing a legitimate interest?
2. Is the processing necessary for that purpose?
3. Do the individual's interests override the legitimate interest?

Further information about conducting this assessment can be found here.

Who is the Information Commissioner's Office (ICO)?

The ICO is

"The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals."

The ICO regulates data protection and associated laws referenced in this guidance, and should be your first stop for definitive guidance about how to implement the GDPR and PECR.

Information register

We have used the term ‘information register’ to refer to a framework for documenting some of your legal obligations and you can find a template at the end of the guidance. There are no hard and fast rules for what this document needs to contain and you might want to amend it so that it suits your needs.

Information sharing agreements

These are also known as data sharing agreements and should document the rules and safeguards to be applied when organisations share personal information with each other. You are likely to need to enter into an information sharing agreement with your school or any other organisation that routinely passes your PTA personal information, especially where it concerns children. Further guidance is available in the data sharing code of practice.

Lawful basis for processing

We have covered these in the guidance. If you require further information to complete your information register, guidance is available here.

Privacy statement

These are sometimes also called privacy notices and are occasionally still referred to as fair processing notices. As we explained earlier in the guidance, you need to provide certain information to people whose information you are processing. Documenting what you are doing with personal information on an information register will help you with this.

Further Information

The ICO has guidance about some topics we have referred to.

The data protection principles

These are not new and underpin existing data protection laws and the GDPR. We have incorporated the principles into this guidance, although it is important that you are aware of them. Under the GDPR, the principles are:

- Lawfulness, fairness and transparency – for PTAs this means that you need to comply with the law and make sure people understand how you process their personal information
- Purpose limitation – this means that you obtain or collect personal information for an explicit, legitimate, and specified purpose (as documented on your information register).You should not use it for any other purpose unless you can demonstrate that it complies with the law
- Data minimisation – this means that you collect the minimum amount of personal information required for your purpose.Don’t collect anything just in case

- Accuracy – where you need to keep personal information, you proactively take steps to make sure it is up to date
- Storage limitation – this means that you only keep personal information for as long as you need it. Don’t keep anything just in case
- Integrity and confidentiality – meaning you have appropriately secured your information and are using appropriate safeguards.Making sure only those that need access to any personal information are able to access it will fall under this principle, as will using passwords and encryption
- Accountability – this means that your PTA can demonstrate that they are complying with data protection laws.

The rights of an individual

Under the GDPR people have the right:

- To be informed – you will be complying with this when you provide them with your privacy statement.
- Of access – if you are processing information about people, they have a right of access to that information. There are not very many situations where you would not be required to give them a copy of their personal information if they ask for it, and therefore you should assume if you are holding personal information about someone, they are entitled to see it. One exception to this rule may be if it contains references to other people – if this happens you should take advice although you should not assume that people are not entitled to it. You also need to be careful with information relating to children. Those with parental responsibility do not have an automatic right to see information that your PTA may hold about their child – you will need to decide whether the child is old enough to understand the consequences and you may require their consent for providing the information. You may also decide that you can only provide the information to the child themselves (assuming they make a request), who may or may not choose to pass the information to those requesting it.
- To rectification – this means that people can ask to have their personal information updated if it is inaccurate or incomplete.If you have passed this information on, for example to a school, you also need to inform them of the changes you have made.
- To erasure – this is also known as "the right to be forgotten" and allows people in certain circumstances to request the deletion or removal of their personal information.If you receive a request and need to comply, don’t forget to make sure their details are removed from every copy of the personal information you may be holding.
- To restrict processing – this may be important to your PTA if you choose to rely on legitimate interests to run hard copy marketing campaigns.You may continue to store data while you investigate but you may not use it for any other purpose. People may ask to restrict processing if their personal information is inaccurate, and you must not process the information until you have checked it is correct.

- To data portability – it is unlikely this will be exercised by members of your PTA. In some circumstances, this right allows people to obtain and re-use their personal data for their own purposes. One example is being able to access and download banking transactions, which people can then use for any purpose they wish to.
- To object – people have a right to object to processing information based on legitimate interests. As with the right to restrict processing, this may be important to your PTA if you are using this for your marketing campaigns. Don't forget – you must inform people about their right to object at "the first point of communication" and in your privacy notice.

People also have rights in relation to automated decision-making including profiling. It is unlikely that most PTAs will need to process these types of request, although it may be important when buying or signing up to online tools. Some of these may use profiling techniques, and may be technically doing this on your behalf. Make sure you look into this further if anything you are signing up to references profiling your system users.

More detailed information about each of these rights is available from the ICO's website here.

Information Register

Type of Information	Purpose of processing1	Lawful basis for processing2	Legitimate interest assessment3	Retention	Access required by	Where is it stored

1 – You should put each different purpose of processing on a separate line.

2 – Your lawful basis should relate specifically to the purpose and therefore you may use a number of different lawful bases for processing the same piece of information. For example, if you want to send marketing to someone's home address you may decide to use consent to do this. If that person is a member of the committee, you will also need to submit their home address to the charity regulator. This is a different purpose and is required by law, therefore the lawful basis for this purpose is a legal obligation.

3 – Only required where your lawful basis for processing is legitimate interests.

This is not legal advice, this is our best interpretation of the current guidance that has been provided by a range of sources.

Reviewed: August 2019