

John Port PTA Data Protection Policy

Adopted at the JPS PTA Committee Meeting 19th June 2018

John Port PTA is a small independent charity, registered with the Charity Commission who use some personal data to communicate with its members. It is a data controller.

Information Register – current personal data used by the PTA

Type of Information	Purpose of processing	Lawful basis for processing	Legitimate interest assessment	Retention	Access required by	Where is it stored
Committee members contact details – telephone numbers and email addresses	To ensure the effective running of the committee	Consent	Yes, it is legitimate	Reviewed each AGM	Committee Members	Secretary's secured personal computer
List of parent volunteers – email addresses	To communicate with a specific group of volunteers who opt in to help the PTA with specific activities	Consent	Yes, it is legitimate	It is reviewed at the start of each school year where volunteers opt in to remain on the list- otherwise they are removed	Secretary	Secretary's secured personal computer
Contact Details on competition forms e.g. Raffle tickets	To contact winners of events	Legitimate Interests	Yes, it is legitimate	Destroyed once the event is complete and the winners notified	Nominated lead for the event	Paper copies held by nominate lead or Secretary personal computer
Students email addresses	Communication to run a specific event	Legitimate interest	Yes, it is legitimate	Removed once event complete	Lead Committee Member	Email software
Cheque details	Photo record of cheque until processed by the bank	Legitimate Interests	Yes, it is legitimate	Photo deleted once bank statement reconciled	Treasurer or their nominee	Treasurer or their nominee

Note: General communications to all the members of the PTA (i.e. all eligible parents, careers, staff, etc.) are sent through the school's communication network (currently Parentmail). The PTA does not have access to these email addresses.

Details of the types of lawful basis for processing data are stated in Appendix 2

How do we collect data ?

We only collect personal data that we need for a specific purpose. We do not collect data 'in case' we might need it. We only hold data for the time that is required and regularly check that it is still required.

We will make it clear why we are collecting someone's data what we are asking them to consent to and how they can withdraw their consent.

Our Privacy statement will be electronically available through the school website and hard copy summary available at any sign-up events.

We communicate directly with volunteers and never ask the school for individual personal information. To be clear the school may send messages from the PTA to the whole school community, but the PTA does not hold this contact information – it is all managed by the school office.

Students' data

Students can work together with the PTA to run an event. This can both be as part of a course project e.g. 6th from BTEC business students running a school disco with PTA support; or extracurricular e.g. supporting the School Council. To facilitate communication, we use student's school email addresses.

Only emails of students directly involved, as proposed by a member of staff, are used. We never use personal email address, we only use a school email address. As a matter of safe guarding the appropriate teacher or member of staff is always copied in on these emails. Communication is limited specifically to the event being run. At the end of the event the PTA committee member removes the students' email address.

What information do we store ?

The personal data we store is summarised in the Information Register contained in this document. Most of the data held is in order to contact people so tends to names, email addresses and some phone numbers.

We do not hold any sensitive personal data (Defined by GDPR as race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life and sexual orientation).

Keeping information safe

Where data is stored electronically we make this 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

- We have one source of contact data held centrally which can be referred to rather than emailing lists of email addresses to people

Where data is stored in hard copy we make this secure by:

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

Social Media

Anyone posting to any of the PTA social media platforms must be aware of what they are posting and any potential implications from both a safe guarding and data protection view. These are public forums which can be accessed by a wide group of people and care must be taken with information posted.

Making data protection a priority

We do not share any of the personal data collected with anyone outside of the PTA and only with relevant members within the PTA as described in the Information Register.

One member of the committee is nominated to lead on data protection and it is always taken into consideration and is 'business as usual'.

Annually, in general around the time of the AGM we will

- Review our Data Protection Policy and the information register to ensure we have a record of what data we are holding and whether we need to add or remove anything from the register.
- Ensure outgoing members destroy any relevant personal data
- Communicate with the list of parent volunteers to gain their consent to remain on the volunteer list

We welcome any sharing of best practise within the PTA community and welcome any audit or investigation by the ICO.

Appendix 1 the GDPR Glossary (taken from the Parentkind website)

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.

You may find it useful to use the ICO's [checklist](#) when preparing your privacy statements.

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](#).

Appendix 2 Legal Basis for Processing (based on advice from ParentKind)

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.