THE PLAY PROFESSIONALS

GDPR

THE PLAY PROFESSIONALS PRIVACY NOTICE:

- We collect information about you when you complete relevant forms, including bookings and registration form and employment and volunteer application form.
- We will use the information about you to administer The Play Professionals services. We will not pass the information about you to any other body without your express permission. Limited, anonymised information may be used by The Play Professionals for analysis of the effectiveness of our services. We will not disclose any information about you to any company other than noted above, or if required to do so by law.
- Marketing: We would like to send you newsletters and other information about our services. If you have consented to receive marketing, you may opt out at a later date. You have a right at any time to stop us from contacting you for marketing purposes.
- You have the right to request a copy of the information that we hold about you and you may ask us to correct or remove information you think is inaccurate.
- Retention of data: once you are no longer involved with The Play Professionals, we will securely retain your data for 3 years for adults and 3 years after a child reaches the age of 18.
- If you have any questions about our privacy policy or information we hold about you, please contact us at **info@playp.org.uk**.

THE PLAY PROFESSIONALS DATA PROTECTION POLICY:

The Trojan Scheme (trading as and here after referred to as The Play Professionals) holds information about parents and children, staff, volunteers and other people involved with our activities.

We have a responsibility to look after this information properly, and to comply with the Data Protection Act. The UK Act was replaced by the EU General Data Protection Regulation (GDPR) from 25th May 2018. The GDPR continues to form the basis of our Data Protection legislation, even once the UK left the EU, so it is fully taken into account in this policy.

Good Data Protection practice is not just a matter of legal compliance and ticking the boxes. Data Protection is about taking care of people and respecting their privacy. Poor practice or a serious breach could not only harm individuals but would also have a serious effect on the reputation of The Play Professionals.

This policy applies to information relating to identifiable individuals which is held by The Play Professionals.

Everything we do with records about individuals – obtaining the information, storing it, using it, sharing it, or even deleting it – will have an acceptable legal basis.

There are six of these:

- Consent from the individual (or someone authorised to consent on their behalf).
- Where it is necessary in connection with a contract between our group and the individual.
- Where it is necessary because of a legal obligation – if the law says you must, you must.
- Where it is necessary in an emergency, to protect an individual's 'vital interests'.
- Where it involves the exercise of a public function – i.e. most activities of most government, local government and other public bodies.
- Where it is necessary in our legitimate interests, as long as these are not outweighed by the interests of the individual.

Where we are basing our processing on consent we will be able to 'demonstrate' that we hold consent. This means having a record of who gave consent, when they gave it, how they gave it (e.g. on the website, on a form, verbally) and what they actually consented to.

In the case of legitimate interests we will do a balancing test, and be confident that our legitimate interests in using the data in a particular way – for example in providing our services or raising funds to support them – are not over-ridden by the interests of the individual.

There are additional considerations where we are holding information about people's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and also genetic data or biometric data, health data or data concerning their sex life or sexual orientation. We will legitimise the use of any of these categories of data by having the individual's explicit consent.

Data Protection compliance is based largely on following six principles:

- Whatever you do with people's information has to be fair and legal. This includes making sure that they know what you are doing with the information about them.
- When you obtain information you must be clear why you are obtaining it, and must then use it only for the original purpose(s).
- You must hold the right information for your purposes: it must be adequate, relevant and limited to what is necessary.
- Your information must be accurate and, where necessary, up to date.
- You must not hold information longer than necessary.
- You must have appropriate security to prevent your information being lost, damaged, or getting into the wrong hands.

We will make key information available to people at the time we collect information from them. This includes:

- The identity and contact details of our group and the person who is responsible for Data Protection;
- The purposes we intend to use the data for and our 'legal basis' for this;
- What we regard as our 'legitimate interests', if this is our basis for processing;

- Any specific recipients of the data or categories of recipients;
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- Details of the individual's rights, such as to request a copy of all the data held;
- The right to withdraw consent if that is the legal basis for processing (but not retrospectively);
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

When a parent or carer registers they know that we will keep a record about them and their activities with us. When a staff member or volunteer joins it's the same. We will therefore tell them anything that may not be entirely obvious to them. This could include any direct marketing that we may want to carry out (see below), or any additional purpose(s) that we might use the data for – publicity, perhaps. ('Data' can include photos, videos, CCTV, audio recordings, etc., not just written records.)

One explicit right that people have is to stop us sending them marketing material (by post, phone, email or text) if they don't want it. When we collect information from people that might be used for marketing we will say so at the time and ask them if they are happy to hear from us. The wording will be along the lines of: "We would like to keep you up to date with information about opportunities and events at The Play Professionals, and how you can support us. Please tick here to indicate which method(s) you are happy for us to use: Mail, Phone, Email, Text Message".

These rules are only for marketing. They do not stop us from contacting people in whatever is the most convenient way to give them information about things they have already signed up to, or for other administrative purposes.

Our activities will be more effective and appropriate if we have good quality records about the people we are working for and with. GDPR insists on this. We will ensure we have the information we need, but no more (it must be adequate, relevant and limited to what is necessary) and it will be as accurate as we can make it and – where necessary – kept as up to date as possible. We will not keep it longer than necessary.

We will remind our staff and volunteers that the individual concerned has the right to see all the information recorded about them by the group. While Data Protection concerns should never prevent us from recording the information we believe we need (especially in cases relating to safeguarding or other serious misbehaviour), being over-casual, rude or injudicious in an email could easily cause a major crisis for The Play Professionals. This can be a useful discipline in deciding what to record and how to record it.

The Play Professionals will also have a clear policy on how long to keep information. We will draw up a retention schedule, taking each type of record we hold and specifying how long we normally keep it, and our justification for this. We will set up a process for ensuring that data is deleted or destroyed routinely at the appropriate time.

THE PLAY PROFESSIONALS

GDPR

We will take good care of the information we hold, whether on computer or on paper, and make sure that we have provided guidance and training to our staff and volunteers so that they treat the information appropriately.

We will think about the risks when data is 'in transit' – either on portable devices or when it is being sent out. For example:

- If people are using their personal phone, laptop, camera or other device for our group's purposes there will be clear expectations of how they should be secured.
- When sending information, particularly by email, we will take steps to prevent confidential information being sent to the wrong person. For example, by using password-protected documents and sending the password in a separate email.
- We will also take care not to disclose people's email addresses or other information inappropriately by carelessly copying in many people or forwarding an email that has been copied widely.
- Information on paper will not be left lying around and will only be taken out of a secure location when this is really necessary.
- Where information is processed for us externally, we will expect the external organisation to be able to give us satisfactory guarantees about the security measures they take.

Responsibility for compliance with Data Protection lies with the organisation, not with any specific individual. The Trustees as a whole body will be responsible to keep up to date with any developments, to check that we are complying and have the evidence to prove it, to give advice to staff and volunteers and to handle any issues such as a data breach or a Subject Access Request. The Trustees may designate someone to be the lead person.

Trustees will be notified in the event of a serious issue eg a data breach.

When we work in collaboration with other organisations we will establish clearly (and in writing) who is responsible for what, in order that there are no Data Protection gaps.

If we engage external suppliers to handle data for us in any way, our contract will set out their responsibilities to handle data in a way that will not cause us to be in breach.

Responsibility for compliance with Data Protection lies with the organisation, not with any specific individual. However, the Trustees may designate someone to lead on: keeping up to date with any developments; checking that we are complying and have the evidence to prove it; giving advice to staff and volunteers and handling any issues such as a data breach or a Subject Access Request.

The individual currently designated is James Jalloh Head of Service.