Making time to listen to children and young people

The Purple Elephant Project
Data Protection Policy
December 2019

This privacy policy describes how The Purple Elephant Project will collect, store, process, share and dispose of any personal data and information provided and are asked to provide for the purposes of our work together as well as your rights in relation to the information collected, processed and shared. The Purple Elephant Project is committed to this policy and places high importance on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all the individuals with whom it deals. We ensure that all employees, agents, contractors, or other parties working on behalf of us comply with these procedures and principles. In order to respond and process any enquiries from you, we require you to agree to the conditions set out in this privacy policy. This statement will be regularly reviewed and updated.
This privacy policy was last updated on 01.12.19.

The named data protection lead at The Purple Elephant Project is: Jenny Haylock, MA and is registered as a Data Controller and Data Processor with the Information Commissioner's Office (ICO), registration number: ZA589845

If you have any questions about this privacy policy please email:
info@thepurpleelephantproject.org

1. The Data Protection Principles
The Data Protection Legislation sets out the following principles with which any party handling personal data must comply. All personal data must be:

- processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
- accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the Data Protection Legislation in order to safeguard the rights and freedoms of the data subject;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

2. The Rights of Data Subjects

The Data Protection Legislation sets out the following key rights applicable to data subjects:

- The right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure (also known as the 'right to be forgotten');
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- rights with respect to automated decision-making and profiling.

3. Lawful, Fair, and Transparent Data Processing

The Data Protection Legislation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the GDPR states that processing of personal data shall be lawful if at least one of the following applies:

- the data subject has given consent to the processing of their personal data for one or more specific purposes;
- the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the data controller is subject;
- the processing is necessary to protect the vital interests of the data subject or of another natural person;
- the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

If the personal data in question is special category personal data (also known as 'sensitive personal data'), at least one of the following conditions must be met:

- the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);
- the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
- the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

- the processing relates to personal data which is manifestly made public by the data subject;
- the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- the processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
- the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;
- the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy)

4. Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

- Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.
- Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.
- Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.
- If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.
- If special category personal data is processed, the Company shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.
- In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that the Company can demonstrate its compliance with consent requirements.

Specified, Explicit, and Legitimate Purposes

- The Purple Elephant Project collects and processes personal data. This includes:
    - personal data collected directly from data subjects; and
    - personal data obtained from third parties.
- The Purple Elephant Project only collects, processes, and holds personal data for the specific purposes set out in our service level agreements.
- Data subjects must be kept informed at all times of the purpose or purposes for which The Purple Elephant Project uses their personal data.

Adequate, Relevant, and Limited Data Processing

- The Purple Elephant Project will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 8, above, and as set out in our Service Level Agreement.
- Employees, agents, contractors, or other parties working on behalf of The Purple Elephant Project may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.
- Employees, agents, contractors, or other parties working on behalf of The Purple Elephant Project may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any unrelated reasons.

Accuracy of Data and Keeping Data Up-to-Date

- The Purple Elephant Project shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.
- The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

Data Retention

- The Purple Elephant Project shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
- When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
- For full details of the Company's approach to data retention, including retention periods for specific personal data types held by The Purple Elephant Project, please refer to our Data Retention Policy.

Secure Processing

The Purple Elephant Project shall ensure that all personal data collected, held, and processed is stored and processed in line with the Data Protection Act (DPA, 1998) and the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) adopted on 27th April 2016 and enforceable from 25th May 2018. Personal data is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

Specifically, this includes:

- All client records, including personal data and sensitive personal data will be held on a secure, GDPR-compliant electronic system.
- Any paper records kept will be kept secure in a locked filing cabinet.
- Any email correspondence from/with you will be uploaded to the secure electronic system and then deleted from the email system.
- Access to your personal information is restricted on a 'need-to-know' basis only, i.e. for those concerned directly with the Service Level Agreement.

All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.
Data security will be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:

a) only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;
b) personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and
c) authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

In the unlikely event of a data protection breach, we will notify the Information Commissioner's Office (ICO) so that the appropriate procedures can be followed.

Accountability and Record-Keeping

- The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.
- All employees, agents, contractors, or other parties working on behalf of The Purple Elephant Project shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Company policies.
- The Purple Elephant Project data protection compliance shall be regularly reviewed and evaluated by means of Data Protection Audits.

Keeping Data Subjects Informed

The Purple Elephant Project shall provide the information set out below to every data subject:

- where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
- where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
- if the personal data is used to communicate with the data subject, when the first communication is made; or
- if the personal data is to be transferred to another party, before that transfer is made; or
- as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

The following information shall be provided in the form of a privacy notice:

- details of the Company including, but not limited to, contact details, and the names and contact details of any applicable representatives and its Data Protection Officer;
- the purpose(s) for which the personal data is being collected and will be processed and the lawful basis justifying that collection and processing;

- where the personal data is to be transferred to one or more third parties, details of those parties;
- details of applicable data retention periods;
- details of the data subject's rights under the Data Protection Legislation;
- details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;
- details of the data subject's right to complain to the Information Commissioner's Office
- where the personal data is not obtained directly from the data subject, details about the source of that personal data;
- where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it

Your Rights

The Purple Elephant Project are fully committed to protecting your rights to privacy. Under the Data Protection Act and General Data Protection Regulations (GDPR), you have certain rights in relation to the personal data collected, stored, processed and shared about you, including the rights to:

- Request access to your personal data.
- Request correction of your personal data.
- Request erasure of your personal data.
- Object to processing of your personal data.
- Request restriction of processing of your personal data.
- Request transfer of your personal data.
- Right to withdraw consent.

If you wish to exercise any of these rights, please contact the Data Protection Lead at The Purple Elephant Project using the contact details at the top of this privacy policy.

Data Subject Access

- Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.
- Employees wishing to make a SAR should do so using a Subject Access Request Form, sending the form to the Company's Data Protection Officer at <<insert contact details>>.
- Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
- All SARs received shall be handled by the Company's Data Protection Officer.
- The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of Personal Data

- Data subjects have the right to require the Company to rectify any of their personal data

that is inaccurate or incomplete.

- The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
- In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

Erasure of Personal Data

Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

- it is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
- the data subject wishes to withdraw their consent to the Company holding and processing their personal data;
- the data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 21 of this Policy for further details concerning the right to object);
- the personal data has been processed unlawfully;

Unless The Purple Elephant Project has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

Restriction of Personal Data Processing

- Data subjects may request that The Purple Elephant Project ceases processing the personal data it holds about them. If a data subject makes such a request, The Purple Elephant Project shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.
- In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Objections to Personal Data Processing

- Data subjects have the right to object to the Company processing their personal data based on legitimate interests, for direct marketing (including profiling)
- Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

- Where a data subject objects to the Company processing their personal data for direct

marketing purposes, the Company shall cease such processing promptly.

Personal Data Collected, Held, and Processed

Full details of the personal data collected, held, and processed by The Purple Elephant Project are available upon request. For details of data retention, please refer to the Company's Data Retention Policy.

Data Breach Notification

- All personal data breaches must be reported immediately to the Company's Data Protection Officer.
- If an employee, agent, contractor, or other party working on behalf of The Purple Elephant Project becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.
- If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer will ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
- In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 18.3) to the rights and freedoms of data subjects, the Data Protection Officer will ensure that all affected data subjects are informed of the breach directly and without undue delay.
- Data breach notifications shall include the following information:
    1. The categories and approximate number of data subjects concerned;
    2. The categories and approximate number of personal data records concerned;
    3. The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
    4. The likely consequences of the breach;
    5. Details of the measures taken, or proposed to be taken, by The Purple Elephant Project to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Implementation of Policy
This Policy shall be deemed effective as of 01.12.19. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name:	Jenny Haylock
Position:	Data Controller and Data Processor for The Purple Elephant Project
Date:	01.12.19
Due for Review by:	01.12.20
Signature:	