DARE's DATA Protection and GDPR Policy

At DARE Playscheme, we collect and process personal information, or personal data, relating to our service users, staff, and workers to manage support and working relationships. This personal information may be held by us on paper or in electronic format. We are committed to being transparent about how we handle personal information, to protecting the privacy and security of personal information and to meeting our data protection obligations under the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018.

We recognise the data protection principles established by GDPR and the Data Protection Act 2018, which provide that personal information we hold must be processed lawfully, fairly and in a transparent manner. It must be collected only for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. It must be adequate, relevant, and limited to what is necessary in relation to those purposes. It must be accurate and, where necessary, kept up to date. It must be kept in a form which permits identification for no longer than is necessary. Personal data must be kept securely and not disclosed orally or in writing, by accident or otherwise, to unauthorised third parties. It must be processed in a way that ensures appropriate security of the data.

Scope
This policy applies to:

- all employees
- workers engaged on a contract for services (sessional workers)
- Directors.

Key responsibilities – staff

- Keep data secure.
- Follow all relevant procedures.
- Report any potential data protection breaches as soon as you become aware of them.

Key responsibilities – managers

- Ensure personal data processed in your area conforms to the requirements of this policy.
- Ensure new and existing staff who are likely to process personal data are aware of their responsibilities and are provided with adequate training and support.

Emails should not be used to transfer personal and special category data unless it is password protected, encrypted or via Egress. We are responsible for, and must be able to demonstrate compliance with, these principles.

Photographs and videos, promotion, and social media

- As part of the registration process, we ensure all parents either consent or refuse consent to taking pictures. The sole use of these pictures is for sharing the activities done during our sessions with parents.
- We do not use these pictures for any form of advertisement or social media.

Any photographs and videos taken by parents/carers at playscheme for their own personal use is not covered by data protection legislation. However, we will ask that photos or videos with other children are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Staff responsibilities

You should always collect and process personal information about people in accordance with the data protection principles, in particular:

- Personal data must be kept securely and not disclosed orally or in writing, by accident or otherwise, to unauthorised third parties.
- If you get data from someone you must inform them appropriately of their rights (i.e. orally or by signposting to a privacy notice)
- Report the loss of any personal or special category data (paper or electronic) or equipment containing such data immediately to your manager.
- Only dispose of personal data by secure destruction and in accordance with the retention schedule
- Take care when discussing staff or service users on phones when others may hear.

DARE Playscheme Data protection by design and default.

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law.
- Completing privacy impact assessments where the playscheme's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the Data controller will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies, and any other data protection matters.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities

DARE Playscheme Data security and storage of records.

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction, or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use. • Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where

there is general access.

- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops, and other electronic devices. Staff and parents are reminded to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.

Staff, or parents who store personal information on their personal devices are expected to follow the same security procedures as for company-owned equipment (see our e- safety policy, ICT policy, mobile phone policy)

Individuals have the right to be informed about the collection and use of their personal data. We use our privacy notices to provide individuals with information, including our purposes for processing personal data, retention periods for that data, and who it will be shared with. The information contained in privacy notices must be provided to individuals and recorded at the time the data is collected from them in a manner appropriate to the data collected and individuals. If we obtain personal data from other sources, privacy information must be provided within a reasonable period of obtaining the data and no later than one month after.

Individuals have the right of requesting access to their data, right to request rectification of errors to their data, right to request the erasure of their data, rights to restricting the processing of their data, right to object to the processing of their data and portability of their data.

Individuals should submit any request to exercise these rights to the Data Controller. If staff receive such a request, they must immediately forward it to the Data Controller. Otherwise, emails need to be sent to tunde@dareplayschemes.co.uk, marked private and confidential for the attention of the Data Controller.

DARE Playscheme response to access requests.

Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected. When responding to requests, we reserve the right to do the following, we:

- We will ask the individual to provide 2 forms of identification.
- We will contact the individual via phone to confirm the request was made.
- We will respond without delay and within 1 month of receipt of the request.
- We will provide the information free of charge.

We tell the individual we will comply within 3 months of receipt of the • request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

We will not disclose information if it:

- Will cause serious harm to the physical or mental health of the client or another individual.
- Will reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.
- Will include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it.
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references.

If the request is unfounded or excessive, we may refuse to act on it, or charge. a reasonable fee which considers administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO. We maintain a registration with the Information Commissioner's Office (ICO)

Nevertheless, in all cases, we will always cooperate with statutory and legal agencies where appropriate.

Data Breaches

We have an obligation to report most personal data breaches to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of that breach. Additionally, if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform individuals affected without undue delay.

As required, the Data controller will set out:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information.
- The Data Controller will submit the remaining information as soon as possible.

A named data controller processes personal data relating to parents, children, staff, visitors,

and others, and therefore is a data controller registered with the ICO and will renew this registration annually or as otherwise legally required. They are responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the board of directors and, where relevant, report to the board their advice and recommendations on data protection issues.

Our Data Controller is Tunde Alabi and is contactable via phone 07743543010 or email tunde@dareplayscheme.co.uk. The Data Controller is also the first point of contact for individuals whose data the playscheme processes, and for the ICO.

There are no International Data transfers.