



DATA PROTECTION POLICY

1. Aims

The Bungalow Partnership aims to ensure that all personal data about children, their families, staff, students, volunteers and other individuals is collected and processed in accordance with the **General Data Protection Regulation (GDPR)** and the expected provisions of the **Data Protection Act 2018 (DPA 2018)** as set out in the **Data Protection Bill**.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA2018. It is based on guidance published by the information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for 'subject access requests'.

3. Definitions

| TERM | DEFINITION |
|-------------------------------------|--|
| Personal Data | Any information relating to an identified, or identifiable, individual. This may include: <ul style="list-style-type: none"> • Name (including initials) • address, D.O.B. • Contact details, email address It may also include factors specific to the individual's physical, psychological, genetic, mental, economic, cultural or social identity. |
| Special categories of personal data | Personal data which is more sensitive and so needs more protection, including information about an individual's <ul style="list-style-type: none"> • Referral information, medical reports, support plans, reviews/reports • SEN, LAC, FSM, • Health care plans, sexual orientation • Ethnicity, religion • Professional body membership, driving licence/passport/liability & car insurance details • Bank details, NI Number, UTR Number, Pension information, • Safeguarding information |
| Processing | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual. |
| Data subject | The identified or identifiable individual whose personal data is held or processed. |
| Data controller | A person or organisation that determines the purposes and the means of processing of personal data. |
| Data processor | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| Personal data breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. |



4. The Data Controller

Our organisation processes personal data relating to children, their families, staff, students, volunteers, trustees and others, and therefore is a data controller.

The organisation is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and Responsibilities

This policy applies to **all staff** employed or otherwise engaged, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 The Board of Trustees

The Board of Trustees has overall responsibility for ensuring that our organisation complies with all relevant data protection obligations.

5.2 Data Protection Officer

The data protection officer (DPO) is 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 trustees and, where relevant, report to the board their advice and recommendations on the organisations data protection issues.

The DPO is also the first point of contact for individuals whose data the organisation processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Marie Blythe and is contactable at The Bungalow Partnership.

5.3 The Director

The Director acts as the representative of the data controller on a day-to-day basis.

5.4 All Staff/Members

Staff/members are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the organisation of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances
 - With any questions about the operation of the policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
 - If they need to rely on a capture consent, draft a privacy notice, deal with data protection rights invoked by an individual
 - If there has been a data breach
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
 - If they need help with any contracts or sharing personal data with third parties



6. Data Protection Principles

The GDPR is based on data protection principles that our organisation must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specific, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the organisation aims to comply with these principles.

7. Collecting Personal Data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law.

- The data needs to be processed so that the organisation can **fulfil a contract** with the individual, or the individual has asked the organisation to take specific steps before entering into a contract
- The data needs to be processed so that the organisation can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the organisation can perform a task in the **public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the organisation or third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely **given clear consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff/members must only process personal data where it is necessary in order to do their jobs.

When staff/members no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with The Bungalow Partnership's Record Retention & Management Policy.



8. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a child, parent/carer or other individual that puts the safety of our staff/members at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers/contractors need data to enable us to provide services to our clients/staff – for example: IT providers, DBS providers. When doing this we will:
 - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
 - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
 - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our such staff/members/clients.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject Access requests and other Rights of Individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that our organisation holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual



'Subject access requests' must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff/members receive a 'subject access request' they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parent/carers of children may be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

Children ages 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents/carers of children may not be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

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

- Might cause serious harm to the physical or mental health of the child or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interest
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administration costs.

A request can 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.



9.4 Other data protection rights of the individual

In addition to the right to make a 'subject access request' (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public health
- Request a copy of agreements under which their personal data is transferred outside the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff/members receive such a request, they must immediately forward it to the DPO.

10. Photographs

As part of our activities, we may take/use photographs and record images of individuals (staff/students/volunteers) within our organisation.

We will obtain consent from individuals for these images and we will clearly explain how the photograph will be used. These uses may include:

- Within our organisation on notice boards and in brochures, newsletters, promotional materials and ID badges
- Online on our website

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph and not distribute it further.

11. Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring that 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 (see section 6)
- Completing privacy impact assessments where the organisation's processing or personal data presents a high risk to rights and freedoms of individuals, and when introducing new techniques (the DPO 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, we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

12. 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 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 office computers, laptops and other electronic devices. Staff/members 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/members who store personal information on their personal devices are expected to follow the same security procedures
- Where personal information needs to be taken off site, staff must ensure it is in a lockable secure container
- Where we need to share personal information with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

13. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example we will shred paper records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on our behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

14. Personal data breaches

The Bungalow Partnership will make all reasonable endeavours to ensure that there are no personal breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches may include, but are not limited to:

- A non-anonymised data being published on our website which shows sensitive information
- Safeguarding information being made available to an unauthorised person



- The theft of therapeutic records (paper copies or electronic on a laptop) containing non-encrypted personal data about clients

15. Training

All staff/members/trustees are provided with data protection training as part of their induction process

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the organisation's processes make it necessary.

16. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the data Protection Bill receives royal assent and becomes law (as the data Protection Act 2018) – if any changes are made to the bill that affect our organisation's practice. Otherwise, or from then on, this policy will be reviewed **every two years** and shared with the Board of Trustees.

17. Links with other policies

This data protection policy is linked to our:

- Freedom of publication scheme