# Data Protection Policy

# (GDPR)

**Approved by Board of Trustees on: June 26th 2018**

**Lead Staff Member: Jackie Rosenberg**
**Lead Trustee: Craig Macdonald**

# Data Protection Policy

**Introduction**

PDT is required to retain certain information about its staff, clients and other individuals to allow it to monitor performance, achievements, security and behaviour and health and safety. It is also necessary to process information so that staff can be paid, projects organised and legal obligations to funding bodies and commissioners met. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, PDT must comply with the Data Protection Principles set out in the General Data Protection Regulation (GDPR) by ensuring that personal information is:

- Obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Adequate, relevant and not excessive for those purposes.
- Accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Processed in accordance with the data subjects rights.
- Kept safe from unauthorised access, accidental loss or destruction.
- Will not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Key features of GDPR include the following:

- Individuals have greater rights over their data
- There are stricter rules on obtaining consent to collect personal data, which must be freely given, specific, informed and unambiguous.
- PDT will need to review our privacy notices and tell individuals the legal basis for processing their information.
- PDT will have to demonstrate compliance with GDPR by and must report any datsa protection breaches.
- PDT will face a significant fine for not reporting a breach of data protection. The maximum fine will increase from £500,000 to £17million in case of a breach.

PDT and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, PDT has reviewed its Data Protection Policy.

**Status of the Policy**
This policy does not form part of the formal contract of employment, but it is a condition of employment that staff will abide by the rules and policies made by PDT from time to time. Any failure to follow the policy can therefore result in disciplinary action.

Any member of staff or volunteer, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the Deputy CE initially. If the matter is not resolved, it should be raised as a formal grievance.

**Notification of Data Held and Processed**
All staff, volunteers and other users are entitled to:

- Know what information PDT holds and processes about them and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what PDT is doing to comply with its obligation under GDPR
- Ask for information to be removed in line with the right to be forgotten.

**Data Security**
All members of staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should be:

- Kept secure, preferably in a locked filing cabinet; or
- In a locked drawer; or
- If it is computerised, be password protected.
- If kept on other media, (e.g. hard disk, USB stick) which is itself kept secure or password protected.

**Rights to Access Information**
Staff, volunteers and other individuals including clients, have the right to access any personal data that is being kept about them by PDT either on computer or in certain organised files. Any person who wishes to exercise this right should complete the PDT Access Request form (Appendix 2).

PDT aims to comply with the requests for access to personal information as quickly as possible, but will ensure it is provided within 20 days, other than in exceptional

circumstances, unless exceptions apply. In such cases, the reason for any delay will be explained in writing to the person making the request.

**Publication of PDT Information**
Information that is already in the public domain is exempt from the 1998 Act. It is PDT policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- Names of PDT Trustees
- Names of PDT staff
- Telephone contact details of PDT offices
- Photographs of PDT staff
- Information about our projects and activities
- PDT's policies and procedures.

**Organisations and Others to which PDT may Provide Data**
PDT may provide data relating to clients to organisations, including but not limited to, Government Departments including the Department for Work and Pensions, local councils, CCGs, Police and auditor. It may also be the case that personal information is provided to such organisations through agencies acting on their behalf.

**Where this the case, PDT will have in place means by which clients give their permission for the sharing of this data.**

**The Processing of personal data**

There are six ways in which the lawful processing of personal data may be carried out. These are where data processing:

- Is necessary for performance of a contract
- Is in compliance with legal obligations
- Is necessary to protect the vital interests of the data subject
- Is in the public interest of exercising of official authority
- Is with the consent of the individual
- Is in the legitimate interests of the controller, or third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual.

**Subject Consent**

***Consent under GDPR must be freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity.***

Some PDT roles will bring the applicants into contact with children, including young people under the age of 19 and vulnerable adults. PDT has a duty under the Children's Act and other enactments to ensure that staff and volunteers are suitable for the job and have the relevant standard or enhanced DBS checks. PDT also has a duty of care to all staff, volunteers and clients and must therefore make sure that employees and volunteers do not pose a threat or danger to other users.

PDT will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. PDT will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency.

**PDT will divulge information on staff and clients without consent if required to do so by law.**

**Processing Sensitive Information**
Sometimes it is necessary to process information about a person's health, criminal convictions, race, sexual orientation, gender re-assignment, religion, marriage / civil partnership, pregnancy / maternity, gender, disability and family details. This may be to ensure that PDT is a safe place for everyone, or to operate other PDT policies such as the sick pay policy or equal opportunities policy.

**CCTV**
PDT operates a number of CCTV cameras in the Stowe Centre in order to assist with the security of the Stowe and protect property and individuals. If any individual has any queries regarding the operation of the CCTV system, they should contact the Facilities Manager at the Stowe Centre. The images are held in secure conditions for 28 days, and on the 29th day they are erased. If anyone wishes to access any personal data about themselves on the CCTV system within 21 days of the occurrence, they should request this of the Facilities Manager with as much information as possible including the reason for their request, to enable the data to be located including, if possible, details of the location of the camera, date and time

**The Data Controller and the Designated Data Controller(s)**
PDT as a corporate body is the data controller under the Act, and the Board of Trustees is therefore ultimately responsible for implementation. However, designated data controllers will deal with day-to-day matters. The first point of contact for any enquiries relating to Data Protection issues should be directed to:

| **Post** | **Area of Responsibility** |
|---|---|
| Head of Community Programmes | For personal information about PDT staff or volunteers |
| Head of Employment | For personal information about Employment Service clients |
| Facilities Manager | CCTV and Security @ Stowe |