Policy Title	**Data Protection Policy**
Policy Owner	**Sarah Perryman**
Version Control	**10**
Review Information	**First Published: May 2018** **Approved: 17/05/2024** **Review Date: 4th March 2025**

Version Control

Version #	Date of review	Reviewer	Summary of changes
10	04/03/2024	Julia Harrison	• Changed font to FS ME Pro • Changed to new headed paper • Added version control box and title box • Added page numbers • Added section headers 1.0-12.0 • Change to the DPO to Emma Jacquest • Amended the Data Request Form.

1.0 Introduction

Tarner is committed to being transparent about how it collects and uses the personal data of individuals, and to meeting its data protection obligations under the General Data Protection Regulations (GDPR) 2020. This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of children and young people accessing Tarner's Children, Youth and Community Projects and their parents/guardians, referred to as service-related personal data. It applies to the personal data of job applicants, employees, workers, trustees, contractors, volunteers, students, former employees, referred to as HR-related personal data. Each of these groups will be provided with a Privacy Notice explaining their own rights as regards this policy.

2.0 Data Protection Officer

The person named as the Data Protection Officer (DPO) with responsibility for data protection compliance within the organisation is the Emma Jacquest. If you have any questions about this policy however, please contact HR@tarner.org.uk in the first instance.

3.0 Definitions

"Personal data" is any information that relates to a living individual who can be identified from that information.

"Processing" is any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

4.0 Data protection principles

Tarner processes personal data in accordance with the following data protection principles as outlined in the GDPR 2020:

- To process personal data lawfully, fairly and in a transparent manner.
- To collect personal data only for specified, explicit and legitimate purposes.
- To process personal data only where it is adequate, relevant, and limited to what is necessary for the purposes of processing.
- To keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- To keep personal data only for the period necessary for processing.
- To adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

At Tarner we tell individuals the reasons for processing their personal data, how we use such data and the legal basis for processing in our privacy notices. We will not process the personal data of individuals for other reasons. Where we rely on legitimate interests as the basis for processing data, we will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where Tarner processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

Tarner will update any out of date personal data promptly if an individual informs their line manager that their information has changed or is inaccurate.

HR-related personal data gathered during the employment of a worker, contractor or volunteer or student is held in the individual's HR personnel file (electronically on SharePoint). Employees of Tarner are responsible for updating their contact details on the HR System, Breathe HR.

Service-related personal data is gathered using a registration form. It is uploaded to our fully GDPR compliant data management system Family for the Children's Project, and Brighton and Hove City Councils ASPIRE CRM for the Youth Project. This is in addition to files found on SharePoint.

The periods for which the organisation holds personal data are contained in its privacy notices to individuals.

Tarner keeps a record of its processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR) including the legal basis for processing the data which are:

- **Consent:** an individual has given clear consent to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract with the individual, or because an individual has asked that specific steps are taken before entering into a contract.
- **Legal obligation:** the processing is necessary for compliance with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.

- **Public task:** the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
- **Legitimate interests:** the processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

5.0 Individual rights

As a data subject, individuals have a number of rights in relation to personal data.

5.1 Subject access requests

Individuals have the right to request information about how their data is being processed as well as access to, and copies of their data. If an individual makes a subject access request, Tarner will tell them:

- Whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- To whom their data is or may be disclosed and the safeguards that apply to such transfers;
- For how long their personal data is stored (or how that period is decided);
- Their rights to rectification or erasure of data, or to restrict or object to processing;
- Their right to complain to the Information Commissioner if they thinks the organisation has failed to comply with their data protection rights; and
- Whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

Tarner will also provide the individual with a copy of the personal data undergoing processing. This request is made electronically, unless is agreed otherwise.

To make a subject access request, individuals must complete a subject access request form (see Appendix 1) and send to HR@tarner.org.uk

Tarner will need to ask for proof of identification before the request can be processed. Tarner will inform the individual the needs to verify their identity and the documents it requires.

Tarner will normally respond to a request within a period of one month from the date it is received, and no administrative charge is made. In some cases, such as where the request involves large amounts of data, Tarner will respond within three months of the date the request is received, and it may incur a small administrative charge. If this is the case, Tarner will advise the individual as soon as possible.

If a subject access request is manifestly unfounded or excessive, Tarner is not obliged to comply with it. Alternatively, Tarner can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify them that this is the case and whether or not it will respond to it.

6.0 Other rights

Individuals also have a number of rights in relation to their personal data. They can require Tarner to:

- Rectify inaccurate data.
- Stop processing or erase data that is no longer necessary for the purposes of processing.

- Stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data).
- Stop processing or erase data if processing is unlawful; and
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether the individual's interests override the organisation's legitimate grounds for processing data.

To ask Tarner to take any of these steps, please contact HR@tarner.org.uk in the first instance.

7.0 Data security

Tarner takes the security of personal data seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where we engage third parties to process personal data on our behalf, such parties do so based on written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

8.0 Impact Assessments

If Tarner processes data which may result in a high risk to an individual's rights and freedoms, we will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

9.0 Data Breaches

If we discover that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery. We will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will also inform affected individuals and provide them with information about its likely consequences and mitigation measures that have been taken.

10.0 International data transfers

The organisation will not transfer personal data to countries outside the European Economic Area.

11.0 Employees responsibilities

Employees are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes his/her bank details.

Some individuals may have access to the personal data of other employees and of our customers and clients in the course of their employment, contract, or volunteer period. Where this is the case, Tarner relies on them to help meet its data protection obligations.

Employees who have access to personal data are required:

- To access only data that they have authority to access and only for authorised purposes.
- Not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation.
- To keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction).

- Not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.
- Not to store personal data on local drives or on personal devices that are used for work purposes; and
- To report data breaches of which they become aware to the HR Manager, immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Tarner's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

12.0 Training

Tarner will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

13.0 Appendices

13.1 Subject Access Request Form
13.2 Service User Privacy Notice
13.3 Employee Privacy Notice

Tarner
Children
Young People
Community

Appendix 1

Data Subject Access Request Form			
By completing this form, you are making a request under the General Data Protection Regulation (GDPR) for information held about you by the organisation that you are eligible to receive.			
Name:		**Daytime Contact Number:**	
Address:		**Email:**	
Required information (and any relevant dates) [Example: Emails relating to "Young person A" between "A" and "B" from 1 May 2021 to 6 September 2021.]			
By signing below, you indicate that you are the individual named above. The organisation cannot accept requests regarding your personal data from anyone else, including family members. We may need to contact you for further identifying information before responding to your request. You warrant that you are the individual named and will fully indemnify us for all losses, cost, and expenses if you are not. **Please return this form to HR@tarner.org.uk** **We will normally respond to your request within 1 month. If your request is complex in nature or involves large amounts of data, we may respond within 3 months. If this is the case, we will inform you as soon as possible.**			
Data Subjects Signature:		**Date:**	