Treasure Your Wellbeing Cic
General Data Protection Regulations (GDPR) Policy

Policy Statement

This regulation is in line with the EU data protection framework 2018. All employees are responsible for compliance and ensuring that personal information maintained is not disclosed orally or in writing or accidentally or otherwise to any unauthorised third party. Any deliberate breach of this policy by any employee may lead to disciplinary action being taken against them. These regulations set out procedures that are to be followed when dealing with personal data. The procedures set out herein are followed by Treasure Your Wellbeing Community Interest Company (TYW CIC), its employees and any other parties working on behalf of TYW CIC. TYW CIC views the correct and lawful handling of personal data as the key to its success and dealings

with third parties and its employees. TYW CIC shall ensure that it handles all personal data correctly and lawfully.

Our data protection principles

All personal data:

- Must be processed fairly and lawfully
- Must be obtained only for specified and lawful purposes and shall not be processed in any manner which is incompatible with those purposes;
- Must be adequate, relevant and not excessive in relation to the purposes for which it is processed;
- Must be accurate and, where necessary, kept up-to-date;
- Must be kept for no longer than is necessary for the purpose(s) for which it is obtained;
- Must be processed in accordance with the rights of data subjects;
- Must be protected against unauthorised or unlawful processing, accidental loss, destruction or damage by the implementation of appropriate technical and organisational measures; and
- Must not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Personal data

Personal data is defined as data which relates to a living individual who can be identified from that data or other information which in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. The regulations also define “sensitive personal data” as personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious (or similar) beliefs; trade union membership; their physical or mental health condition; their sexual life; the commission or alleged commission by them of any offence; or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Employees’ personal data

TYW CIC only holds personal data that is directly relevant to its employees. That data will be held and processed in accordance with the data protection principles and with these regulations. The following are examples of data which may be collected, held and processed by TYW CIC:

Identification information relating to employees including, but not limited to, names and contact details;

Equal opportunities monitoring information including age, gender, race, nationality and religion;

Health records including details of sick leave, medical conditions, disabilities and prescribed medication;

Employment records including, but not limited to, interview notes, curricula vitae, application forms, assessments, performance reviews and similar documents;

Details of salaries

Records of disciplinary matters including reports and warnings, both formal and informal

Details of grievances including documentary evidence, notes from interviews, procedures followed and outcomes

Other person's personal data

Information relating to individuals will be obtained for the delivery of services. This could include confidential information such as names, addresses, personal circumstances, credit or debit card details, bank details etc. Care is taken to ensure that the information being obtained is adequate, relevant and not excessive for the purpose for which it is intended to be used. The information will not be processed or stored in any manner incompatible with that purpose. The information will be kept safe from unauthorised access, accidental loss or destruction, and will not be maintained for longer than is necessary.

Access to data

Employees and other individuals that TYW CIC hold information about have the right to access any personal data maintained about them electronically or in paper files. The application must be made in writing, and they maybe required to provide additional identity information. Upon

receipt of a Subject Access Request, TYW CIC shall have a maximum period of 30 days within which to respond.

Data breach

TYW CIC will notify the relevant authority of data breaches where appropriate. This will be done without undue delay, and where feasible, within 72 hours of awareness. TYW CIC will provide a reasoned justification if this timeframe cannot be met. Where relevant, the Directors will also notify the affected data subject without undue delay. Additionally, TYW CIC will also contact the UK ICO in the event that a serious breach has occurred. TYW CIC will ensure that procedures are adopted internally for handling data breaches in all cases.