

# The Yogi Group

## Data Protection Policy

### **1. Policy Aims**

The Yogi Group (also referred to as TYG Ltd.) is committed to protecting the rights and freedom of all individuals in relation to the processing of their personal data. This policy covers the collection, use, storage and sharing of data relating to The Yogi Group's business, staff and clients, whether stored electronically or in paper format.

The purpose of this data protection policy is to outline the acceptable code of conduct for persons working with, for or under the name of TYG Ltd., and to provide guidance for best practice in relation to data usage.

### **2. Information we collect**

TYG Ltd. may collect and process the following types of personal information:

- Contact Information, e.g. Name, email address, phone number, postal address.
- Identification information for staff / contractors.
- Disclosure and Barring Service information for staff / contractors.
- Cookies or other similar technologies.

Other data may be collected where it is deemed necessary, and will be stored, used and destroyed according to the Data Protection Act 2018, the UK GDPR and in accordance with the 6 principles in the policy statement below.

### **3. How we use data:**

TYG Ltd. may use personal information for the following purposes:

- To provide and maintain our services.
- To communicate with clients/staff about products, services, and promotions.
- To ensure safety and safeguarding within our services.
- To improve our services.

### **4. Scope**

TYG Ltd. must comply with the Data Protection Act 2018 and UK General Data Protection Regulations (UK GDPR). This policy has been developed to ensure all staff, contractors and partners understand their obligations when processing data.

This policy and the legislation apply to all personal data, both that held in paper files and electronically. If the processing of the data is carried out for purposes relating to TYG Ltd.'s business, staff or clients, it applies regardless of where the data is held.

'Processing' data is widely defined and includes obtaining, recording, keeping, or using data in any way; sharing or disclosing it; erasing and destroying it.

All staff, contractors and partners must ensure they process data according to the Data Protection Act 2018, the UK GDPR and in accordance with the 6 principles in the policy statement below.

## **5. Policy Statement**

All personal and special category data must be:

### **5.1. Processed lawfully**

All personal and special category data must be processed lawfully, fairly and in a transparent manner in relation to individuals.

### **5.2. Used for specific purpose**

The data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

### **5.3. Be relevant to the purpose**

The data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

### **5.4. Be accurate**

Data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

### **5.5. Kept no longer than is necessary**

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals

### **5.6. Kept Securely**

Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

## **6. Data Security**

Keeping personal data properly secure is vital in complying with the Data Protection Act. All staff and contractors are responsible for ensuring that any personal data we have access to is kept securely. We are also responsible for ensuring that personal data is not disclosed inappropriately (either orally or in writing or accidentally) to any unauthorised third party.

This includes, as a minimum:

- Keeping passwords safe and never sharing them.
- Keeping personal data kept in paper format stored securely.

## **7. Prohibited Activities**

The following activities are strictly prohibited when processing personal and special category data:

- Sending data to unauthorised personnel. Always check that the recipients are authorised to view the information being sent
- Sending personal data in an insecure format
- Losing or misplacing personal and sensitive data
- Leaving personal data unprotected
- Accessing personal data about an individual for personal use
- Disclosing personal data to a third party without a lawful basis

### **7.1. Implications of breaching this policy**

It is a condition of employment in the case of staff, contractors and partners of TYG Ltd. that they abide by the law and the policies of TYG Ltd. Any breach of this policy may be considered a disciplinary offence and may lead to disciplinary action. A serious breach of the Data Protection Act 2018 may also result in TYG Ltd. and/or the individual being held liable in law.

## **8. Exemptions**

Exemptions to the Data Protection Act 2018 can apply in a small number of areas and only where the restriction respects the essence of the individual's fundamental rights and freedoms and it is a necessary and proportionate measure in a democratic society to safeguard:

- National security;
- Defence;
- Public security;
- prevention, investigation, detection or prosecution of criminal offences;

- Other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- Breaches of ethics in regulated professions;
- Monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- The protection of the individual, or the rights and freedoms of others; or
- The enforcement of civil law matters

## **9. Acknowledgement and Agreement**

Please contact [theyogigroup@gmail.com](mailto:theyogigroup@gmail.com) if you have any concerns about our data protection practices.



Laura Mitchell

Director of TYG Ltd.

REVIEW 31.08.24