Data Protection Policy

Policy Statement

Rubix Consulting takes its responsibilities with regard to the management of the requirements of the General Data Protection Regulation (GDPR) very seriously.

The organisation is committed to being transparent about how it collects and uses the personal data of its workforce, clients and delegates and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

Rubix Consulting obtains, uses, stores and otherwise processes personal data relating to potential staff and students (applicants), current staff and students, former staff and students, current and former workers, contractors, website users and contacts, collectively referred to in this policy as data subjects. When processing personal data, the Organisation is obliged to fulfil individuals' reasonable expectations of privacy by complying with GDPR and other relevant data protection legislation (data protection law).

Data Protection Principles

The organisation processes HR-related personal data in accordance with the following data protection principles:

1. The Organisation processes personal data lawfully, fairly and in a transparent manner
2. The organisation collects personal data only for specified, explicit and legitimate purposes
3. The organisation processes personal data only where it is relevant and limited to what is necessary for the purposes of processing
4. The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
5. The organisation keeps personal data only for the period necessary for processing
6. The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage

Data Breaches

If the organisation discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 48 hours. The Organisation 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, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

Individual Responsibilities

1. Individuals 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
2. Individuals may have access to the personal data of other individuals and of our customers and clients during their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff and to customers and clients
3. Individuals who have access to personal data are required:
    a. to access data for authorised purposes only
    b. to only access data they have the authority to access
    c. to keep data secure (by complying with procedures on computer access, password protection, file storage etc)
    d. not to disclose data, expect to individuals who have appropriate authorisation
    e. not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without implementing appropriate security measures (for example, password protection) to secure the data and the device
    f. to not store personal data on local devices

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

Additional Data Protection Principles for delegates attending TW Courses

Information we may collect from you:

- Information you provide when submitting your personal details (for example, on our Booking Form and Joining Instructions);
- Publicly available information about yourself;
- Record of correspondence from yourself;
- Details about your dietary and access requirements as well as any reasonable adjustments or special requirements for events; and
- Equality and diversity information

What we may use your data for:

- Communication with yourself about booking or application;
- Assisting in the preparation of the event or programme;
- Evaluating and analysing the information provided by you including for diagnostics and for speakers to prepare for the programme/event they are to deliver;
- To deal with any queries or complaints in relation to your attendance at an event or programme; and
- Generating reports for internal use by us (including our staff) in relation to your attendance at an event or programme.
- As required by CITB, Rubix Consulting must maintain and retain reliable documentation for quality assurance purposes. Your details will form a part of these records and will be used to audit course delivery.
- When requested by CITB, Rubix Consulting will share your personal information with CITB.

Where we wish to use data for other purposes, we may anonymise your information so that it cannot be linked to you. In which case, it will cease to be personal data and we may use the anonymised data for any purpose.

How we will protect your personal information

- We are committed to securely holding your personal information
- Where personal information is held electronically, it is held on a computer system that is owned and controlled by Rubix Consulting or such other third party appointed by Rubix Consulting
- Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access
- We are required (by CITB guidelines) to retain your information for a minimum of 3 years for quality assurance and audit purposes

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Umbreen Munir PhD BSc (Hons)

January 2021

Signed | Print Name | Date