****

Data Protection Policy

# September 2021

## 1. Introduction

The Retrofit Academy CIC (TRA) is committed to ensuring that any data relating to staff, learners or anyone internal or external to the activities of RTA is protected under the General Data Protection Regulations (GDPR). This is a statement of the data protection policy adopted by TRA.

TRA needs to collect and use certain types of information about the individuals or users of its services, who need to be in contact with TRA so that it can carry out its work. These include current, past, and prospective employees, professional experts, delegates, individual employers, and others.

This personal information must be collected and dealt with appropriately whether it is received on paper, stored in a computer database, or recorded on other material, so there are safeguards to ensure this under General Data Protection Regulations (GDPR).

## 2. Scope

This policy concerns information relating to living, identifiable individuals. This policy applies to all The Retrofit Academy employees’ and those individuals working on behalf of The Retrofit Academy (i.e., Moderators, External Quality Assurers, Internal Quality Assurers and other consultants).

## 3. Purpose

TRA is committed to being transparent about how it collects and uses the personal data of its workforce, centres/individuals at centres, other customers/clients, learners, employers, contractors or other personal data processed for business purposes, and to meeting its data protection obligations. This policy sets out the TRA's commitment to data protection, and individual rights and obligations in relation to personal data.

TRA has appointed Jenny Pierpoint, Chief Operating Officer, as the person with responsibility for data protection compliance within the organisation. She can be contacted at jenny@retrofitacademy.org. Questions about this policy, or requests for further information, should be directed to her.

## 4. Definitions

‘Personal data’ is any information that relates to an 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.

## 5. Data protection principles

TRA processes personal data in accordance with the following data protection principles:

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

TRA advises individuals on the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where TRA 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.

TRA will update personal data promptly if an individual advises that their information has changed or is inaccurate.

TRA keeps a record of its processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

## 6. Individual rights

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

### 6.1 Subject access requests

Individuals have the right to make a subject access request.

TRA will normally respond to a request within a period of one month from the date it is received. In some cases, such as where TRA processes a large amount of an individual's data, it may respond within two months of the date the request is received. TRA will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, TRA is not obliged to comply with it. Alternatively, TRA 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 TRA has already responded. If an individual submits a request that is unfounded or excessive, TRA will notify the indivisual that this is the case and whether it will respond to it.

If TRA can respond to a subject access request, it will inform the individual:

* 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, including to recipients located outside the European Economic Area (EEA) 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 think TRA has failed to comply with their data protection rights; and
* Whether or not TRA carries out automated decision-making and the logic involved in any such decision-making.

TRA will also provide the individual with a copy of the personal data processed. Unless requested otherwise, the response will be provided in an electronic format.

If the individual wants additional copies, TRA will charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies. To make a subject access request, the individual should send the request to jenny@retrofitacademy.org. In some cases, TRA may need to ask for proof of identification before the request can be processed. TRA will inform the individual if it needs to verify their identity and the documents it requires.

### 6.2 Other rights

Individuals have a number of other rights in relation to their personal data. They can require TRA 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 TRA’s legitimate grounds for processing data (where TRA 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 TRA's legitimate grounds for processing data.

To ask TRA to take any of these steps, the individual should put the request in writing to jenny@retrofitacademy.org.

## 7. Data security

TRA takes the security of personal data seriously and has 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 TRA engages third parties to process personal data on its behalf, such parties do so on the basis of 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. Impact assessments

Some of the processing RTA carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, TRA 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. Data breaches

If TRA discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. TRA 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.

## 10. International data transfers

Where TRA is obliged to transfer personal data the UK, i.e., to or from international centres the data will be transferred in adherence with GDPR.

## 11. Individual responsibilities

Individuals are responsible for helping TRA keep their personal data up to date. Individuals should let TRA know if data provided to TRA changes. Individuals 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 personal data or that can be used to access personal data, from TRA's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
* Not to store personal data on local drives, or on personal devices that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the TRA’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. Training

TRA 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.

This policy will be updated as necessary to reflect best practice in data management, security, and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulations (GDPR).

.

If you would like to feedback any views, please contact us via the details provided below.

### Contact us

Anyone who would like to feedback on this strategy, or have any queries about its content, please contact us on:

T: 0330 055 7629

E: info@retrofitacademy.org

### Related Policies

* Complaints policy.
* Appeals policy and procedures.
* Any other policy that may give rise to a breach of data protection.