Data Protection Policy

1. Policy statement

1.1. This policy defines how R&R Recruitment (R&R), intends to deliver the enhanced rights of the General Data Protection Regulation 2018 (GDPR) for workers in line with the legislation developments of the Data Protection Bill (DPB) that amends the Data Protection Act 1998 (DPA).

1.2. This policy outlines the standards we require workers to observe when collecting, storing and processing personal and sensitive data and how the Training Centre will communicate the activity to those individuals and how the Training Centre will monitor and what action will be taken in respect of breaches of this policy.

1.3. This policy may be amended at any time and changes will be communicated accordingly.

2. Who is covered by the policy?

2.1. This policy covers all workers.

3. The scope of the policy

3.1. This policy covers all workers including the Board, all employees, consultants, agency workers and volunteers (collectively referred to as **workers** in the policy.)

3.2. It applies to all data that the Redirct Traffic Management. The following terms are used throughout this document:

1. **Data Controller** determines the purposes and means of processing personal data.
2. **Data Processor** is responsible for processing personal data on behalf of a data controller.
3. **Data Subject** which is a living individual who the personal data is identifiable to.

3.3. Personal data is any information relating to a person who can be identified, directly or indirectly, either by an 'identifier' such as their name, or an identification number, or by location or online data, or through factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

3.4. Special category data is defined as data which include sickness absence/medical information, equal opportunities monitoring information.

3.5. Breach of this policy may be dealt with under the Redirct Traffic Management Disciplinary & Capability Procedure and, in serious cases, may be treated as Gross Misconduct and result in summary dismissal and be reported to the Information Commissioners Office (ICO).

4. Responsibility for implementation of the policy

4.1. R&R Recruitment's Director has overall responsibility for the effective operation of this policy.

4.2. The Data Protection Working Group (inclusive of the Finance Director, IT Manager, HR Manager and Legal & Insurance Manager) are responsible for reviewing this policy and making recommendations for changes to minimise risks to the rights and freedoms of those working for Mac Projects international training centre and prevent enforcement action that can damage both the Company reputation and impact the Company financially.

4.3. All workers are responsible for their own compliance with this policy and for ensuring that it is consistently applied. All workers should ensure that they take the time to read and understand it. Any breach of this policy should be reported to their line manager and then to the Legal & Insurance Manager.

4.4. Questions regarding the content or compliance of this policy should be directed to the Legal & Insurance Manager, who will act as the representative for the Training Centre for any data subjects and for the regulator the ICO.

4.5. The IT Manager is responsible for ensuring all systems, services and equipment used for storing data meet acceptable security standards. Also responsible for regular performance checks and scans to ensure security hardware and software is functioning properly. Then the evaluation of any third party services the Company is considering using to store or process data.

4.6 The Marketing Manager is responsible for approving any data protection statements attached to communications such as emails and letters. As well as working with workers to ensure marketing initiatives abide by data protection principles.

5. Data protection principles

5.1. The Data Protection Bill (DPB) requires that all workers and others who process or use any personal information must ensure that they adhere to the **6 data protection principles** set out by the DPB. In summary these require that personal data, including sensitive data to be;

1. obtained and processed in a transparent manner, fairly and lawfully.
2. the data held is accurate and kept up to date.
3. is adequate, relevant and not excessive for those purposes.
4. not kept longer than required necessary.
5. is stored safely from unauthorised access, accidental loss or destruction.
6. is processed for the specified, explicit or legitimate purposes of collection.

6. Worker's Rights

6.1. Data subjects have the;

1. (a) right to be informed about the processing of their personal data.
2. (b) right to rectification if their personal data is inaccurate or incomplete (requests to amend data to be processed within one month).
3. (c) right to access their personal data and supplementary information, and the right to confirmation that their personal data is being processed.
4. (d) right to be forgotten by having their personal data deleted or removed on request where there is no compelling reason for the Training Centre to continue to process it (requests will be responded to without reasonable delay and within one month of the request).
5. (e) right to restrict processing of their personal data, for example, if they consider the processing to be unlawful or the data inaccurate.
6. (f) right to data portability for their own purposes (they will be allowed to obtain and reuse their data).
7. (g) right to object to the processing of their personal data for direct marketing, scientific or historical research, or statistical purposes.

7. Consent

7.1 R&R Recruitment will continue to reply on expressed consent from its learners and workers to process for example medical records where necessary for preventative or occupational medicine, assessing working capability or confirming medical diagnosis.

7.2. Where consent is given, the learner or worker is entitled to then retract their consent at any given time and this will be adhered to by the Company.

8. Privacy Notices (PN)

8.1. All current and prospective learners and workers will receive a PN to inform them of how the Company intends to process their personal data.

8.2. Any changes to the way data is processed, or the type of data collected workers will be communicated to accordingly.

8.3. The PN will outline how the R&R Recruitment lawfully process a learner or worker's personal and special category data in order to;

1. Perform the employment contract.
2. Comply with a legal obligation.
3. Protect the worker's or another individual's vital interests (for example during a medical emergency).
4. Carry out a task in the public interest, or in exercising official authority vested in the employer.
5. Protect the legitimate interests of the employer or third party, except where this is overridden by the interests or rights of the worker.

9. General Guidelines

9.1. The only learner or worker able to access data covered by this policy should be those who need it for their work.

9.2. Data should not be shared informally. When access to confidential information is required, workers can request it from their line manager.

9.3. RTM will provide training to all employees to support understanding of their responsibilities when handling data.

9.4. Strong passwords must be used and they should never be shared.
9.5. Personal data should not be disclosed to unauthorised learners and workers, or those external to the RTM

9.6. Personal data will be regularly reviewed and updated if it is out of date, and no longer required, it will be deleted and disposed of confidentially using the Training Centres confidential waste bins or shredders.

9.7. Workers should request support from their line manager or Human Resource Department if they are unsure about any aspect of data protection.

10. Data Storage and Security

10.1. RTM requires all learners and workers to store both electronic and paper data in a safe, secure manner to avoid unauthorised access, accidental deletion and malicious hacking attempts.

10.2. Data stored on paper when not required, the paper or files should be kept in a secure place i.e. a locked drawer or filling cabinet where unauthorised people cannot see it.

10.3. Learners and workers should make sure paper and printouts are not left out where unauthorised people could see them, like on a printer.

10.4. Data printouts should be shredded or disposed of securely when no longer required using the confidential waste bins at each depot.

10.5. Electronic data should be protected with strong passwords that are changed regularly and never shared between workers.

10.6. If data is stored on a removable media (for example a CD or DVD) these should be kept locked away securely when not in use.

10.7. Data should be stored on designated drives and servers (in your departments' folder within the Training Centre File) and should only be uploaded to an approved cloud service.

10.8. RTM servers containing personal data are sited in a secure location, away from general office space.

10.9. RTM data is backed up frequently and the backups are tested annually in line with The Training Centres backup procedure.

10.10. Workers should never save other learners or workers personal data directly to their laptops or other mobile devices like tablets or smart phones.

10.11. All the RTM servers and computers containing data are protected by approved security software and a firewall.

10.12. RTM will conduct 'Data Protection Impact Assessments' (DIPA) to identify and minimise that data the potential protection risks of a project.

11. Data Protection Impact Assessment

11.1. RTM are required under the GDPR to take a risk based approach to compliance, therefore completing a DPIA before carrying out processing that is likely result in high risk to individual's interests.

11.2. The DPIA will assess the level of risk, considering both the likelihood and the severity of any impact on individuals i.e. the specific nature, scope, context and purposes of the processing.

11.3. RTM will carry out a new DPIA if there is a change in the nature, scope, context or purposes of our processing.

11.4 If the DPIA identifies a high risk which Training Centre cannot mitigate, the Legal & Insurance Manager will consult the ICO.

12. Data usage

12.1. Personal data when accessed and used can be at risk of being lost, corrupted or stolen therefore when working with personal data;

1. Learners and workers should ensure the screens of their electronic devices i.e. computers, laptops, mobile phones, PDAs etc. are always locked when left unattended.
2. Personal data should not be shared informally. Therefore learners and workers must not send personal data to their personal email.
3. Data must be encrypted before being transferred electronically, please seek support from the IT Manager to send data to authorised external contacts.
4. Personal data should never be transferred outside of the European Economic Area.
5. Learners and workers should not save copies of personal data to their electronic devices i.e. computers, laptops, mobile phones, PDAs etc.

13. Data Accuracy

13.1. The law requires RTM to take reasonable steps to ensure personal data is kept accurate and up to date, therefore it is the responsibility of the workers to ensure;

1. Personal data will be held in as few places as necessary. Learners and workers should not create unnecessary additional data sets.
2. Learners and workers should take every opportunity to ensure data is updated. For example, by confirming a customer's details when they call or when inaccuracies are discovered.
3. Learners and workers should use the 'Change of Personal Details Form' located on the intranet under the Human Resource Department/Employment to ensure the data is correct.
4. Currently MailChimp Email Software supports the Marketing Manager to maintain CRM databases.

14. Data Retention

14.1 Personal data will not be retained any longer than required by RTM.

14.2. All Department Managers who process personal data are required to produce a data schedule and review on an annual basis.

15. Monitoring at Work

15.1. RTM reserves the right to monitor quantity and quality of work produced by their workers. Monitoring is also carried out to safeguard workers and our customers. Please refer to our 'Acceptable Usage Policy' for further information.

15.2. RTM uses systematic and occasional monitoring to monitor workers performance and conduct. Systematic describes regular monitoring and occasional is when there is concern raised that requires to be investigated.

15.3. The types of monitoring used are as follows:

1. Individual email addresses may be accessed and/or telephone conservations listened to, when there is a requirement to investigate due to allegations of misconduct or cause for concern regarding a workers' performance.
2. Additional to the above worker's emails and recording of telephone calls may be accessed for training purposes or in event of a customer complaint.
3. Email filters have been applied to all worker's email accounts to flag any use of inappropriate language in their email communication.
4. Website filters have been applied and appropriate blocks to certain websites where the content is regarded as inappropriate by the Company i.e. pornography or gambling sites.
5. Systematic checking of telephone logs for numbers called to detect premium-rate numbers.

6. Those workers who have access to Company vehicles are subject to systematic vehicle tracking and telematics technology which may include use of tachographs and video footage within the cabs of their vehicles.
7. The Training Centre operates CCTV cameras for security purposes however also reserves the right to access the CCTV and use as evidence when there is an allegation of misconduct.

16. Subject access requests procedure

All individuals who are the subject of personal data held by MPITC entitled to:

1. Ask what information the Company holds about them and why.
2. Ask how to gain access to it.
3. Be informed how to keep it up to date.
4. Be informed how the Company is meeting its data protection obligations.
5. If an individual contacts the Company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email to or alternately by letter addressed to the Human Resource Department. An individual will not be charged a fee for a data subject request unless the request is 'manifestly unfounded or excessive' (for example repeat request from the same individual) and in these circumstances the Company will charge a reasonable fee or may refuse to act on the request. The Human Resource Department will without delay and within one month provide the relevant data. However an extension may be granted of two months if necessary, when taking into account of the complexity of the request. All individuals will have their identity verified prior to information from the subject access request being handed over.

17. Sharing and transferring personal data

17.1. RTM is responsible to ensure a third party such as a recruitment agency is compliant with GDPR through the review of their contract terms.

17.2. RTM will also need to share some personal data with Awarding Organisations (AO's) such as Lantra or other accredited AO's that we use to deliver qualifications.

18. Disclosing data for other reasons

18.1. In certain circumstances, personal data will to be disclosed to the emergency services without consent of the data subject i.e. worker.

19. Breaches

19.1. All data protection breaches must be reported to the Legal & Insurance Manager who will then document on the 'Data Protection Breach Log' within 24 hours of becoming aware of the breach by completing the 'Data Protection Breach Notification Form'.

19.2. When there is a likelihood the breach could result in risk to the rights and freedoms of individuals the Legal & Insurance Manager will notify the ICO.

19.3. Notification of this type of breach will be made within 72 hours of the Company becoming aware of the breach.

19.4. When breaches are identified as high risk then individuals will be notified without delay.

20. Monitoring and review of this policy

20.1. The policy will be reviewed when necessary to ensure that it meets legal requirements of data processing to identify and limit any detrimental effects of data processing on individual privacy.

Jordan Storer

Managing Director

Date: 16 March 2022

ISSUE DATE;	04-12-2020	Author; Jordan Storer	Authorised by; Jordan Storer
Reviewed;	15-07-2021	Changes; Jordan Storer	Authorised by; Jordan Storer
Reviewed;	16-03-2022	Changes; Jordan Storer	Authorised by; Jordan Storer
13/06/2022; COMPANY NAME CHANGE.		Changes; Jordan Storer	Authorised by; Jordan Storer
Review due;	16-03-2023		
Reviewed;	13-03-2023	Changes; Aimee Owen	Authorised by; Jordan Storer
Review due;	13-03-2024		