DATA PROTECTION POLICY

DATA PROTECTION POLICY

1 AIMS

Melton Accident Repair Centre Limited (MARC) (referred to as 'the provider') collects and uses personal information about staff, users and other individuals who come into contact with the provider. This information is gathered in order to enable the provider to provide body shop services for our users and other associated functions e.g. employment. In addition, there may be a legal requirement to collect and use information to ensure that the provider complies with its statutory obligations.

2 WHY HAVE THIS POLICY

This Policy sets the providers obligations regarding the collection, processing, transfer, storage, and disposal of personal information. The procedures and principles set out herein must be followed at all times by the provider, its employees, board members, agents, contractors, or other parties working on behalf of the provider.

MARC is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the UK General Data Protection Regulation (UK GDPR) and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

3 DEFINITIONS

UK GDPR
The UK General Data Protection Regulation (UK GDPR) is a regulation in UK law on data protection and privacy for all individuals within the United Kingdom. It also addresses the export of personal data outside the UK

Personal Data
The UK GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Special Categories of Personal Data
The UK GDPR defines "Special Categories" of Personal Data as any information relating revealing racial or ethnic origin, political opinions, religious or philosophical beliefs. Trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is also classed as "Special Categories" of Personal Data.

Data Subject
A data subject is an individual who is the subject of personal data. For example, Shopmobility hold personal data about service users, making each service user a data subject under the terms of the UK GDPR.

Data Protection Officer
Role required by the General Data Protection Regulation. Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with UK GDPR requirements.

Data Controller
The Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Processor
A data processor is distinct from the data controller for whom they are processing the personal data. An employee of a data controller, or a department or unit within the provider which is processing personal data. The processor maybe a third party with which the provider has a GDPR compliant contract.

Data Breach
A data breach is an incident that involves the unauthorized or illegal viewing, access, retrieval, accidental deletion or not proper use of data by an individual, a provider, application or service.

4 WHAT WE DO AND WHO DOES IT

MARC processes personal information relating to users, staff and visitors and, therefore, is a data controller. MARC is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

MARC Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring the providers compliance with the UK GDPR. The DPO would also work with MARC by providing guidance and to develop related policies. They will report to the highest level and liaise with the ICO as and when required.

The directors have overall responsibility for ensuring that the provider complies with its obligations under the General Data Protection Regulation. On a daily basis, responsibilities lie with the Data Controller. In the absence of the Data Controller the Lead Processor will take up the role. The Data Protection Officer and the Data Controller will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform MARC of any changes to their personal data, such as a change of address.

5 PERSONAL DATA WE COLLECT

MARC will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) This includes personal data collected directly from data subjects. MARC only collects, processes, and holds personal data for the specific purposes (or for other purposes expressly permitted by the UK GDPR). Data subjects are kept informed at all times of the purpose or purposes for which the provider uses their personal data.

Users

We hold personal data about users to support their requirements and to assess how the provider is performing.

This data includes, but is not restricted to:

- Contact details
- Safety information (first aid, incidents)

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected. We will not share information about users with anyone without consent unless the law and our policies allow us to do so. We are required, by law, to pass certain information about service users so that they are able to meet their statutory obligations.

Staff

We process data relating to those we employ to work at, or otherwise engage to work at, the provider. The purpose of processing this data is to assist in the running of the provider, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Ensure that we have relevant information for medical emergencies, next of kin contact etc.

Staff personal data includes, but is not restricted to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures
- Appraisal information
- Contact information for next of kin

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected. We will not share information about staff with third parties without consent unless the law allows us to. We are required, by law, to pass certain information about staff to specified external bodies, so that they are able to meet their statutory obligations. Any staff member wishing to see a copy of information about them that the provider holds can contact the office of the Data Protection Officer, the Subject Access Request (SAR) procedure must be followed.

6 DATA PROTECTION PRINCIPLES

This Policy aims to ensure compliance with the UK GDPR. The UK GDPR sets out the following principles with which any party handling personal data must comply. The controller shall be responsible for and be able to demonstrate, compliance with the principles.

All personal data must be:

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 the data subject.
- 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.

7 OUR COMMITMENT

MARC is committed to maintaining the data protection principles at all times. Therefore, the company will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

8 LAWFUL, FAIR, AND TRANSPARENT DATA PROCESSING

At MARC we ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The UK GDPR states that processing of personal data shall be lawful if at least one of the following applies:

- The data subject has given consent to the processing of their personal data for one or more specific purposes;
- The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data.

9 THE RIGHTS OF DATA SUBJECTS

At MARC the Data Controller is the responsible for allowing data subjects to exercise their rights and to ensure that they can make effective use of them. The UK GDPR sets out the following rights applicable to data subjects:

The right to be informed
In order to ensure that personal data are processed fairly, data controllers must provide certain minimum information to data subjects, regarding the collection and further processing of their personal data. The UK GDPR adds that such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The right of access
Data subjects have the right to file a subject access request (SAR) and obtain from the data controller a copy of their personal data, together with an explanation of the categories of data being processed, the purposes of such processing, and the categories of third parties to whom the data may be disclosed.

The right to rectification
Data subjects have the right to require the data controller to correct errors in personal data processed by (or on behalf of) that controller.

The right to erasure
Allows data subjects to require data controllers to delete their personal data where those data are no longer needed for their original purpose, or where the processing is based on the consent and the data subject withdraws that consent (and no other lawful basis for the processing exists).

The right to restrict processing
To restrict processing is a new right created under the UK GDPR. In certain circumstances in which the relevant personal data either cannot be deleted (e.g. because the data are required for the purposes of exercising or defending legal claims) or where the data subject does not wish to have the data deleted, the data controller may continue to store the data, but the purposes for which the data can be processed are strictly limited.

The right to data portability
This permits the data subject to receive from the data controller a copy of his or her personal data in a commonly used machine-readable format, and to transfer their personal data from one data controller to another or have the data transmitted directly between data controllers.

The right to object
Data subjects continue to have a right to object to processing of their personal data on certain grounds

The rights with respect to automated decision-making and profiling
The rights related to automated decision making and profiling. The UK GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

10 HOW WE STORE DATA

Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal information are kept secure when not in use. We carry out visual audits and regularly improve our practices.

- All records are stored in a central location. This is locked and only certain staff have access to these.
- Papers containing confidential personal information should not be left on office desks or pinned to notice boards where there is general access.
- Where personal information needs to be taken off site (in paper or electronic form), staff must ensure this is secure. Confidential data can only be taken out with the approval of the senior management team.
- Passwords that are secure are used to access the providers computers, laptops and other electronic devices.
- All electronic data information systems are password protected.
- Staff are reminded to change their passwords at regular intervals
- No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the provider where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the UK GDPR (which may include demonstrating to the provider that all suitable technical and organisational measures have been taken).
- Encryption software is used to protect all portable devices and removable media, such as USB devices Staff who store personal information on their personal devices are expected to follow the same security procedures for provider-owned equipment.

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. At MARC we have adopted this approach when we

- are installing or adopting new ICT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- working with a new supplier that involves sharing
- using data for new purposes.

11 DATA ACCURACY

Data held will be as accurate and up to date as is reasonably possible. Every opportunity will be given to the data subject to update the information the provider holds. If a data subject informs the provider of a change of circumstances their computer record will be updated as soon as is practicable.

A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the provider will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Directors for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

12 WHO WE SHARE DATA WITH

We will not share information about users with anyone without consent unless the law and our policies allow us to do so. We are required, by law, to pass certain information about staff to specified external bodies, so that they are able to meet their statutory obligations.

We do use information such as names to create passwords and login details for approved ICT systems but never share contact details with such companies. Other agencies and professional bodies may include but not limited to:

- Auditors for MARC
- Police forces, courts, tribunals- when we are legally bound to do so.

We will not share information about staff with third parties without consent unless the law allows us to. We are required, by law, to pass certain information about staff to specified external bodies, such as HMRC so that they are able to meet their statutory obligations. Any staff member wishing to see a copy of information about them that the company holds should contact the organisations Data Protection Officer.

13 ACCOUNTABILITY AND RECORD KEEPING

The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the provider's other data protection-related policies, and with the UK GDPR and other applicable data protection legislation. MARC shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information.

- The name and details of the provider, its Data Protection Officer, and any applicable third-party data processors;
- The purposes for which the Company collects, holds, and processes personal data;
- Details of the categories of personal data collected, held, and processed by the provider, and the categories of data subject to which that personal data relates;
- Details of any transfers of personal data to non-UK countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by the provider (please refer to the Data Retention Policy); and
- Detailed descriptions of all technical and organisational measures taken by the provider to ensure the security of personal data.

14 DATA RETENTION

MARC shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

For full details of the providers approach to data retention, including retention periods for specific personal data types held by MARC, please refer to our Data Retention Policy.

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

15 SUBJECT ACCESS REQUESTS

A Subject Access Request (SAR) enables individuals to find out what personal data you hold on them, why you hold it and who you disclose it to. The UK GDPR enforces strict parameters on the way these requests are dealt with. Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

Following the UK GDPR's guidelines all requests will be responded to without delay and at the latest, within one month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request. Where a request is manifestly unfounded or excessive, the provider holds the right to refuse to respond to the request.

The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal. In the event that a large quantity of information is being processed about an individual, the provider will ask the individual to specify the information the request is in relation to. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format. If the request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

SAR Procedure

- Data Subject or their Representative makes a request in writing to the provider
- MARC reply and request data subject to complete Subject Access Request Form
- MARC to verify the identity of the person making the request the following are accepted as evidence of identity:

  Passport
  Driving licence
  Utility bills with current address
  Birth / Marriage certificate
  P45/P60
  Credit Card or Mortgage statement

- The request is logged by MARC. If the initial request does not clearly identify the information required, then further enquiries will be made. The response time for subject access requests, once officially received, is 30 days. However, the 30 days will not commence until after receipt of clarification of information sought.

- The provider provides the information in line with the request

It must be noted any information which may cause serious harm to the physical or mental health or emotional condition of the service user or another should not be disclosed, nor should information that would reveal that the service user is at risk of abuse, or information relating to court proceedings. If there are concerns over the disclosure of information then additional advice should be sought. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained.

If information contained within the disclosure is difficult to read or illegible, then it should be retyped. Information can be provided at the provider with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

16 DATA BREACH

In the case of a data breach, the person causing or noticing the breach should log the breach with the Data Protection Officer and the Data Controller

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of service user, staff or trustee data and/ or equipment on which data is stored;
- Unauthorised use or Access;
- Equipment Failure;
- Poor data destruction procedures;
- Human mistake;
- Cyber-attack;
- Hacking.
- Unforeseen circumstance such as fire or flood;
- Data not fully used or acted up on.

In most cases, the next stage would be for the DPO to fully investigate the breach. The DPO and/or team leader should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

The type of data;

- Is it sensitive;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (service users, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency. On reviewing the breach The Data Protection Officer or the Data Controller should not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with UK GDPR, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

17 TRAINING

Our staff are provided with UK GDPR training as part of their induction process. UK GDPR training will also form part of continuing professional development, where changes to legislation or the company's processes make it necessary. MARC will ensure the senior management team fully understand UK GDPR and its potential impact. All other staff are trained according to their roles and responsibilities. We stress how the UK GDPR is the responsibility of the whole company.

18 CONTACT DETAILS AND USEFUL WEBSITES

Data Protection Officer

TBA

Data Controller

Melton Accident Repair Centre
8 North Street,
Melton Mowbray
LE13 1NL

Useful Websites

www.ico.org.uk

www.gov.uk

www.leicestershire.gov.uk

19 REVIEW

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Data Protection Officer or nominated representative.