Document history			
Issue Level	**Page No(s)**	**Date**	**Brief details of amendment(s) to this document**
1	All	05/07/18	First issue of GDPR manual

1.0 Purpose

1.1 To detail how Roocroft Road Restraint Systems Ltd reviews and evaluates compliance with the General Data Protection regulations (GDPR).

1.2 To ensure continued compliance with the general the Data Protection Act 1998 & the General Data Protection regulations 2018.

1.3 To provide employees and subjects with information on how data is obtained, processed and disposed of.

1.4 Roocroft Road Restraint Systems Ltd are a data controller.

2.0 Related Documents

2.1 The General Data Protection Regulations (GDPR) 2018

2.2 The Data Protection Act 1998

2.3 GDPR General Guidance

2.4 Data Protection Impact Assessment

2.5 GDPR Audit Report Form

3.0 Responsibility

3.1 The person responsible for control of data is the Operations Director/SHEQ Manager.

3.2 All members of staff are responsible for ensuring they follow correct data collection and handling procedures as detailed within this manual.

3.3 The Data controller is responsible for ensuring any third party involved in data collection or processing adheres to the General Data Protection Regulations (GDPR) 2018 and The Data Protection Act 1998.

4.0 Data Protection Policy

Roocroft Road Restraint Systems Ltd are committed to preserving the privacy of its learners and employees and to complying with the Data Protection Act 1998 and the General Data Protection regulations 2018. To achieve this commitment information about our learners, employees and other clients and contacts must be collected and used fairly, stored safely and not unlawfully disclosed to any other person.

Roocroft Road Restraint Systems Ltd are registered with the ICO as data handlers. The nominated Data Protection Coordinator has operational responsibility for the implementation of this policy. The Directors hold overall responsibility for data protection. All Managers and Staff (whether employed or contracted) are responsible for ensuring that any personal data which they hold is kept securely and personal information is not disclosed in any way and to any unauthorised third party.

All Managers, staff and others who process or use any personal information must ensure that they follow the data protection principles set out in the Data Protection Act 1998 and the General Data Protection Regulations 2018. These are that personal data shall:

- Be obtained with the explicit consent of the subject.
- Be obtained and processed fairly and lawfully.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept longer than is necessary for that purpose.
- Be processed in accordance with the data subject rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic area, unless that country has equivalent levels of protection for personal data.
- No personal data will be released to third parties except to relevant statutory bodies. In all other circumstances the consent of the individuals concerned must be given and documented before releasing personal data.

Control Measures to be followed at all times:

- All personal data to be stored in lockable cupboards.
- Not left on unattended desks or tables.
- Unattended ICT equipment should not be accessible to other users - Use the screen lock on laptops and PC's.
- ICT equipment used off-site must be password-protected.
- Data files on CD or memory stick or email attachments used off-site containing personal data must be password-protected.
- Paper records containing personal data must be shredded where appropriate.
- Staff must not disclose personal data to any individual, without authorisation or agreement from the data controller.
- Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated data controller.
- Only the Wifi password for the Guest Network is to be shared and no access shall be granted to the general company Wifi system

Signed: Joint Managing Director

Dated: 05/07/18

Roocroft Road Restraint Systems Ltd will make the Data Protection Policy publicly available by clearly displaying on the organisations website and displaying in the reception area.

Organisation Name's Data Protection Policy is reviewed on an annual basis and re-affirmed by the Board of Directors.

5.0 Purpose for data collection

5.1 Roocroft Road Restraint Systems Ltd collect and process data for the purpose of:

- **ROOCROFT ROAD RESTRAINT SYSTEMS LTD:** 'The provision of risk analysis, method statements, collaborative sharing for ISO standards and sharing of RAMS with partner organisations and principle contractors. Additionally, personnel data of those who work directly for or who are sub-contracted to the organization.

5.2 No personal data will be collected for any other purpose.

6.0 Means of consent

6.1 The main changes / enhancements on requirements form the Data Protection Act 1998 under the GDPR is that consent should be **"unambiguous" and given "by a statement or by a clear affirmative action".**

6.2 Data is collected by means of an opt-in process where explicit consent is provided by the following means:

- Contact forms via website
- Inbound enquiries via email (responses to email will contain an opt out action)
- Inbound telephone calls (calls will be recorded, and affirmation obtained)
- Direct marketing where subjects pass contact details (initial contact will be by either telephone & recorded or by email that will contain an opt out action)

Telephone consent – the following statement should be given during a recorded conversation
"all calls are recorded for training and quality purposes"
Email consent – always use company email account with the optout statement in the footer of the message.
Web contact forms – will contain the statement "by clicking submit I agree this information to ROOCROFT ROAD RESTRAINT SYSTEMS LTD for the purpose of obtaining services provided by the ROOCROFT ROAD RESTRAINT SYSTEMS LTD and agree to my contact information being retained on file" "ROOCROFT ROAD RESTRAINT SYSTEMS LTD will only hold data for the purposes of providing services to clients. We will not share any data with any other entity unless legally obliged to do so"

7.0 Rights to Data Protection Under the GDPR

7.1 Subjects have the following rights under the GDPR

- The right to request access to data held about them
- The right to be forgotten (deletion of all data relating to them)
- The right to be informed
- the right to rectification of data held
- the right to restrict processing
- the right to data portability
- the right to object and rights in relation to automated decision making and profiling.

7.2 There are other more specific rights available to some subjects for further information on these specific rights please refer to page 4 “Conditions for special categories of data” of the GDPR General Guidance document.

8.0 Process for Dealing with Data Requests Under the GDPR

8.1 All requests for access to data should be referred to the Data Controller.

8.2 The Data Controller will record the request on the Data Protection Impact Assessment spreadsheet REQUESTS tab detailing the following information:

Name	Nature of Request	Date	Action Taken	Any changes to procedures?	Date Action Taken	Subject Happy?
J Blogs	General enquiry as to what data is held	01/12/17	Copy of info held on database provided – subject happy with data held	None	10/12/17	Yes

8.3 All requests must be responded to within 30 days of receipt.

9.0 Data Protection Impact Assessment

9.1 ROOCROFT ROAD RESTRAINT SYSTEMS LTD will undertake a Data Protection Impact Assessment that will address the following information:

Data Asset	Owner	Location	Consent Method	Risk Description	Impact Description	Before Controls				Additional or Mitigating Measures to reduce Risk / Impact	After Controls			
						L	S	R	P		L	S	R	P
XXXXXXXX	XXXXXXXX	XXXXXXXX	email web form telephone	XXXXXXXX	XXXXXXXX	3	5	15	Medium	XXXXXXXX	1	5	5	Low

9.2 ROOCROFT ROAD RESTRAINT SYSTEMS LTD will review control measures and if necessary implement additional controls and document them on the Data Protection Impacts Assessment.

9.3 The Data Controller will ensure that a review of the Data Protection Impacts Assessment is undertaken on an annual basis and make any amendments as necessary to maintain adequate control over personal data.

10.0 Data Collection & Storage Process

10.1 ROOCROFT ROAD RESTRAINT SYSTEMS LTD will ensure the following controls are implemented and maintained:

10.2 **Records of consent**

- telephone (recorded consent)
- email (opt-in opt-out options)
- web forms (opt-in on form)

10.3 **Storage methods**

- Microsoft Outlook
- CRM system database

- HiHi Telephone System
- Online ePortfolio System
- Any personal data will be stored on the company Network Drive or cloud hosted with access rights/control strictly monitored.

10.4 **Access restrictions**

- Encrypted email system in use
- Password protected database
- Password protected CRM database system

10.5 **Updating of data**

- All staff are responsible for notifying any changes to contact data. The administration & sales teams are responsible for ensuring information is updated with any changes

10.6 **Retention times**

- Financial transactions 7 years (required by law)
- Customer data

10.7 **Use of personal data from a third party** will be checked before use for:

- TPS listing
- Evidence of consent from provider
- Subjects will be given the option of opt-out of future correspondence

11.0 Third Party Data Collection & Storage

11.1 ROOCROFT ROAD RESTRAINT SYSTEMS LTD will assess the systems in place by any third-party data controller to ensure they are in compliance with the GDPR, affirmation of compliance must be received in writing and held on record.
11.2 Details of confirmation of consent from the subject obtained shall be held on file.
11.3 Details of compliance will be added to the Data Protection Impact Assessment.

12.0 Data Destruction Process

12.1 ROOCROFT ROAD RESTRAINT SYSTEMS LTD will ensure any personal hard copy data is shredded and disposed of by a licenced waste / data destruction contractor.
12.2 Copies of destruction certificates will be obtained and held on file.
12.3 Electronic data will be permanently deleted – all copies of data will also be deleted

13.0 Data Protection Breaches

13.1 ROOCROFT ROAD RESTRAINT SYSTEMS LTD Group will record all data breaches, investigate the cause and detail action(s) taken to report the data breach and prevent recurrence.

Date	Nature of Breach	Reportable (who to)	Action(s) Taken	Date Action Taken
01/12/17	Customer database hacked by unknown party	ICO - also contacted all customers that are on the database to reassure them the only data obtained was Name & Tel No	IT Support traced issue to insecure firewall - upgraded patch & changed to a more secure password	03/12/17

14.0 Training & Awareness

14.1 ROOCROFT ROAD RESTRAINT SYSTEMS LTD provide training to all employees in data protection
14.2 Providing all employees with access to this GDPR Manual
14.3 Providing online training in data protection
14.4 Issuing data protection guidelines in the company employee handbook

15.0 Compliance

15.1 ROOCROFT ROAD RESTRAINT SYSTEMS LTD will undertake an annual review of the Data Protection Policy
15.2 ROOCROFT ROAD RESTRAINT SYSTEMS LTD will undertake an annual audit of data protection arrangements

16.0 Further Guidance

Data protection | Privacy and Electronic

At-a-glance guide to the marketing rules

Method of communication	Individual consumers (plus sole traders and partnerships)	Business-to-business (companies and corporate bodies)
Live calls	☐ Screen against the Telephone Preference Service (TPS) ☐ Can opt out	☐ Screen against the Corporate Telephone Preference Service (CTPS) ☐ Can opt out
Recorded calls	☐ Consumer must have given caller specific consent to make recorded marketing calls.	☐ Consumer must have given caller specific consent to make recorded marketing calls.
Emails or texts	☐ Consumer must have given sender specific consent to send marketing emails/texts. ☐ Or soft opt-in (previous customer, our own similar product, had a chance to opt out)	☐ Can email or text corporate bodies ☐ Good practice to offer opt out ☐ Individual employees can opt out
Faxes	☐ Consumer must have given sender specific consent to send marketing faxes	☐ Screen against the Fax Preference Service (FPS) ☐ Can opt out
Mail	☐ Name and address obtained fairly ☐ Can opt out	☐ Can mail corporate bodies ☐ Individual employees can opt out

ico. Information Commissioner's Office

20180307
Version 2.2

Information Commissioner's Office - 0303 123 1113

Roocroft Road Restraint System Ltd. Registered in the name of: David Roocroft

"These rules on consent, the soft opt-in and the right to opt out ***do not apply to electronic marketing messages sent to 'corporate subscribers'*** *which means companies and other corporate bodies eg limited liability partnerships, Scottish partnerships, and government bodies. The only requirement is that the sender must identify itself and provide contact details."* ***And provide an opt out mechanism.***

What you cannot do is send joebloggs@yahoo.co.uk or another@gmail.com an email unless they opt in because that is classed as private.

Business-to-business texts and emails

GDPR Update

If you are processing an individual's personal data to send business to business texts and emails the right to object at any time to processing of their personal data for the purposes of direct marketing will apply. The right to object to marketing is absolute and you must stop processing for these purposes when someone objects.

See our right to object guidance for further details.

142. These rules on consent, the soft opt-in and the right to opt out do not apply to electronic marketing messages sent to 'corporate subscribers' which means companies and other corporate bodies eg limited liability partnerships, Scottish partnerships, and government bodies. The only requirement is that the sender must identify itself and provide contact details.

143. However, it serves little purpose to send unsolicited marketing messages to those who have gone to the trouble of saying they do not want to receive them.

144. Corporate subscribers do not include sole traders and some partnerships who instead have the same protection as individual customers. If an organisation does not know whether a business customer is a corporate body or not, it cannot be sure which rules apply. Therefore we strongly recommend that organisations respect requests from any business not to email them.

145. In addition, many employees have personal corporate email addresses (eg firstname.lastname@org.co.uk), and individual employees will have a right under section 11 of the DPA to stop any marketing being sent to that type of email address.

What information you must supply	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller and where applicable, the controller's representative and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.	✓	✓
When should information be provided?	At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month) If the data are used to communicate with the individual, no later than the date when the first communication takes place; or If disclosure to another recipient is envisaged, no later than before the data are disclosed.

Area of Data Protection	Evidence	Compliant Y/N
Is the data controller identified?		
Has the Data Protection Policy been reviewed & is it still relevant?		
is the reason why data is obtained still relevant?		
How is consent obtained and is this still relevant?		
Have there been any changes to the rights to access data? (see GDPR)		
Have any requests been made & if so have these been recorded?		
Is the Data Protection Impact Assessment complete & reviewed?		
Is the data collection & storage (section 10) process being followed?		
Have any 3rd party data holders been assessed / any new data holders?		
Are data retention times in place and being followed?		
Is the data destruction process being followed		
Have there been any data breaches and if so have they been recorded & investigated?		
Is the PCI certificate in date?		

ROOCROFT ROAD RESTRAINT SYSTEMS

GDPR AUDIT REPORT FORM
(Lead sheet)

Page 1 of ___

Audit No	Auditor	Date	Date closed

Problem Report No(s)	**Audit summary:**
	Auditee Signature **Date**

Corrective Action (fix now)

Corrective/Preventive Action (if required)

Date of Follow-up Audit
Result of Follow-up Audit

Evaluated for similar non-conformances?		Details:
Any changes required to risk analysis?		

Auditor **Date**