HANDLING PERSONAL DATA POLICY

1. Introduction

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in our organisation and will provide for successful business operation. We are firmly committed to protecting the confidentiality and integrity of the Personal Data of our customers, suppliers, employees, workers and other third parties.

From 25 May 2018, our data processing activities will be governed by the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPRs"). We have put in place a number of procedures and safeguards to protect the Personal Data we hold and Process.

2. Terminology

The GDPRs refer to a number of different terms. For the purpose of the GDPRs, we are the 'Data Controller' of all personal data obtained by us, because we ultimately determine how that personal data will be handled by us or any of our sub-contractors, who would be our 'Data Processors'. As we primarily supply our products to businesses and distributors, rather than individual consumers, the amount of personal data we obtain is limited. However, we still need to be mindful of our obligations when Processing this data.

When we handle personal data of individuals, even individuals with whom we deal in a business capacity, then those individuals are "Data Subjects". This means they have certain rights under the GDPRs in relation to how their personal data is processed.

"Personal Data" is any information that can be used to identify a Data Subject, including their name, e-mail address, IP address, or any other data that could reveal their identity.

"Processing" is any operation performed on Personal Data, such as collection, recording, storage, retrieval, use, combining it with other data, transmission, disclosure or deletion.

If we Process the Personal Data of a Data Subject, then we must issue them with a "Privacy Notice". This is a document describing how we collect and process personal data and it must contain various specific information under the GDPRs. These can be general (such as on our website), or specific if the Processing is related to a specific purpose.

"Sensitive Data" would be classified as (1) special category data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, biometric (e.g. fingerprints or facial recognition) or genetic information or information about a person's health or (2) data relating to criminal convictions or offences (including allegations).

3. Compliance with this Policy

This Policy sets out the standards we require from anyone handling Personal Data and compliance is mandatory. It applies to all employees, workers and contractors. This Policy does not form part of your contract of employment or engagement, nor does give rise to any contractual rights to any customer or third party.

Anyone who fails to comply with this Policy may be subject to disciplinary action or the termination of their engagement, as appropriate. You should also be aware that the Company could be exposed to significant fines and reputational damage if Personal Data is not treated lawfully. In certain circumstances you could have personal liability under data protection law for data breaches.

The Quality Manager is responsible for overseeing this Policy and our compliance generally with data protection laws. Please contact them with any questions you have on this Policy or if you have concerns that it is not being followed.

4. Data Protection Principles

We adhere to the data protection principles set out in law when Processing Personal Data. These are:

1. **Lawful and fair processing**. We must identify a lawful ground for collecting and Processing Personal Data and Process based on that purpose.

2.	**Transparency.** Individuals must be told how and why we are Processing their Personal Data, who we would share it with and how long we will retain it.
3.	**Purpose Limitation:** We must only collect Personal Data for a specific, explicit and legitimate purpose. Any subsequent Processing should be compatible with that purpose, unless the Company obtained the individual's consent or the processing is otherwise permitted by law.
4.	**Data Minimisation:** We must only Process Personal Data that is adequate, relevant and limited to what is necessary for the purpose for which it was collected.
5.	**Data Accuracy:** We must take reasonable steps to ensure Personal Data is accurate and kept up to date.
6.	**Storage Limitation:** We must only keep Personal Data for as long as it is needed for the purpose for which it was collected or for a further permitted purpose.
7.	**Data Security and Integrity:** We must have in place appropriate technical and organisational measures to protect Personal Data from unlawful or unauthorised Processing.
8.	**Transfer Limitation:** We must not transfer Personal Data to another country without appropriate safeguards being in place.
9.	**Individual Rights and Requests:** We must allow individuals to exercise their rights in relation to their Personal Data, including their rights of access, erasure, rectification, portability and objection.

As a Data Controller, we are responsible for demonstrating compliance with these principles.

5. What you are required to do

In order to ensure that the data protection principles are adhered to, we have put in place certain compliance requirements.

Ensure processing is fair and for a specific purpose

Data protection law allows Processing for specific purposes, and the grounds which will be most commonly used in our business are:

(a) the individual has given his or her consent;

(b) the Processing is necessary for the performance of a contract with the individual;

(c) to meet our legal compliance obligations.;

(d) to protect the individual's vital interests;

(e) to pursue our legitimate interests for purposes where they are not overridden by the rights and freedoms of the individual.

We must identify and document the legal ground being relied on for each Processing activity.

We cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the individual of the new purposes and they provided consent where necessary. Our Privacy Notice sets out why we are Processing Personal Data, and you must only Process Personal Data as instructed by your line Manager.

Be transparent when dealing with Data Subjects

Whenever we collect Personal Data directly from individuals, we must provide them with the information required by law including the identity of the Company as Data Controller, how and why we will use, Process, disclose, protect and retain that Personal Data. This must be presented when the individual first provides the Personal Data. Generally, the Privacy Notice on our website will contain the required information. With respect to our staff, the Employee Privacy Notice sets out the required information.

When Personal Data is collected indirectly (for example, from a third party or publically available source), we must provide the individual with all the information required by law as soon as possible after collecting/receiving the data. We must also check that the Personal Data was collected by the third party in accordance with applicable data protection laws and on a basis which contemplates our proposed Processing of that Personal Data.

If you are in any doubt as to whether the Privacy Notice on our website or Employee Privacy Notice applies to the Processing that you are carrying out please contact the Quality Manager.

Process data only when you have a need to do so

You may only Process Personal Data when it is necessary in the course of performing your job duties. You cannot Process Personal Data for any reason unrelated to your job duties.

Ensure data is accurate

Personal Data must be accurate and, where necessary, kept up-to-date. It must be corrected or deleted without delay when inaccurate. You inform the Quality Manager if you consider that Personal Data is inaccurate or out-of-date and you must always obtain their approval prior to destroying or amending it. No data should be amended or deleted without prior approval. If you are asked by the Quality Manager to amend or delete data then you must do so without delay.

Adhere to our retention policies

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. It is your responsibility to ensure you are familiar with our retention policies and that you take all reasonable steps to comply with them.

Assist the Company with security integrity and confidentiality

Protecting Personal Data

We will develop, implement and maintain safeguards appropriate to our business, the amount of Personal Data that we own or maintain on behalf of others and identified risks. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

You must follow the procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPRs and relevant standards to protect Personal Data.

Reporting a Personal Data Breach

The GDPRs requires Data Controllers to notify any data breach to the applicable regulator and, in certain instances, the individual.

We have put in place procedures to deal with any suspected breach of Personal Data and will notify individuals or any applicable regulator where we are required to do so.

If you know or suspect that a breach of Personal Data has occurred, do not attempt to investigate the matter yourself. Immediately contact the Quality Mangaer. You should preserve all evidence relating to the potential breach.

6. Sharing Personal Data

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with third parties, such as our service providers if they need to know the information for the purposes of providing the contracted services and we have an agreed contract in place with them which ensures that they will comply with the GDPRs. You must also not share Personal Data with third parties without the approval of the Quality Manager.

Please note that there are specific rules on transferring Personal Data outside of the European Economic Area ("EEA") (whether that it to a group company or a third party). If you believe you need to share Personal Data with anyone that is based outside the EEA then you must obtain prior approval from the Quality Manager.

7. Direct Marketing

We are subject to certain rules and privacy laws when marketing to our customers and contacts.

For example, an individual's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the individual in an intelligible manner so that it is clearly distinguishable from other information and you must use the Company's standard wording for all marketing communication.

An individual's objection to direct marketing must be promptly honoured. If a customer or contact opts out at any time, this information should be passed to the Operations Manager as soon as possible.

8. Children's Data

Under the GDPRs, there are specific rules relating to the Processing of Personal Data of children (those under 13 years of age). It is highly unlikely that we would come into contact with any Personal Data of children. However, if you know or suspect we are going to handle personal data in relation to children you must inform the Quality Manager.

9. Individual's rights and requests regarding their Personal Data

Individuals have rights when it comes to how Data Controller's handle their Personal Data. These include rights to:

(a) withdraw consent to Processing at any time;

(b) receive certain information about the our Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(i) object to decisions based solely on Automated Processing, including profiling;

(j) prevent Processing that is likely to cause damage or distress to them or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority; and

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party.

You must immediately forward any request you receive from an individual relating to their Personal Data to the Quality Manager.

Under no circumstances should you attempt to deal with a request yourself or disclose Personal Data to anyone without prior authorisation.

10. Privacy By Design and Data Protection Impact Assessments

We will implement appropriate technical and organisational measures to ensure compliance with data privacy principles. As a business, we are all responsible for continually considering whether any measures can be implemented on our programs, systems and processes to protect Personal Data. If you have any suggestions, please let the Quality Manager know.

A Data Protection Impact Assessment (DPIA) must be completed in respect to high risk Processing.

You should ask the Quality Manager to conduct a DPIA as part of implementing any major system or business change programs involving the Processing of Personal Data including:

(a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(b) automated processing including profiling and automated decision making;

(c) large scale Processing of Sensitive Data; and

(d) large scale, systematic monitoring of a publicly accessible area (such as CCTV).

11. Training and Audit

Training will be given to all personnel who might have access to Personal Data which will be appropriate to their role.

We will regularly review all the systems and processes we have in place to ensure they comply with the Data Protection Principles and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data. If you believe that there any changes to our systems or processes are necessary in order for us to protect Personal Data, you should inform the Quality Manager as soon as possible.

12. Changes to this Data Protection Policy

We will periodically review this Policy, along with all supporting documents and guidelines we have to do with data protection compliance, to ensure that they continue to comply with the relevant legal requirements. In the event that we make any changes we will notify you of them.