Purpose

The purpose of this policy is to outline the Company's policy regarding the processing, protecting and maintaining of personal and confidential data. This policy is in accordance with the Data Protection Act 1998 and the General Data Protection Regulation (EU) 2016/679 (GDPR), the purpose of which is to protect the rights and privacy of individuals, and to ensure that data about them are not processed without their knowledge.

Scope

This policy applies to electronic and paper records containing personal data. It also covers data held on all employees of the Company. All customers, consultants, suppliers and subcontractors, along with anyone who may process personal data on behalf of the Company, are required to strictly adhere to this policy.

Policy Statement

The company holds and processes important information about employees, customers, consultants, suppliers and subcontractors. This information includes, but is not solely limited to, contact details, bank accounts and payment details. The Company recognises the importance of handling such sensitive information and how the management of this data affects the individuals concerned.

Through this Data Protection policy, the Company endeavours to ensure that the information held on its systems is kept secure and accurate.

The Company and all staff are committed to fully complying with the principles set out in the General Data Protection Regulations:

1. Lawfulness, fairness and transparency

Transparency: We will inform the subject what data processing will be done. **Fair:** What is processed will match up with how it has been described. **Lawful:** Processing will meet the tests described in GDPR [article 5, clause 1(a)].

2. Purpose limitations

Data will only be used for specific processing purposes that the subject has been made aware of and no other, without further consent.

3. Data minimisation

Data collected on a subject will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In other words, no more than the minimum amount of data will be kept for specific processing.

4. Accuracy

Data will be accurate and where necessary kept up to date.

5. Storage limitations

Data will be stored for no longer than is necessary, after which time it will be removed from our systems.

6. Integrity and confidentiality

We will handle data in a manner ensuring appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage.

Security

All employees must ensure that they follow the laid down security procedures for handling data to ensure there is no unauthorised disclosure.

Any employee found accessing personal data that they are not entitled to see will be subject to disciplinary action.

Responsibilities

The Managing Director has overall responsibility for this policy.

Company Responsibilities:

The Company has a responsibility to ensure that personal data dealt with in the course of the Company's business is handled in accordance with the GDPR provisions and reasonable steps will be taken by all concerned to ensure this duty is observed.

The Company will take such measures as may be necessary to ensure the proper training, supervision and instruction of all relevant employees in matters pertaining to data protection and to provide any necessary information.

Staff Responsibilities:

All employees must ensure that the personal information that they provide to the Company in connection with their employment is accurate and up to date.

If an employee believes that the data held on them is inaccurate they should contact their line manager in the first instance who will ensure that their records are properly updated.

On an annual basis the Company will make available to the employee the information that they hold for that individual. It is the employee's responsibility to advise the Company of any amendments to this data. The Company shall not be held responsible for errors of which it has not been informed.

Rights of Access

Data subjects will have the right to:

- access and obtain a copy of their data on request;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing their data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of their data where the organisation is relying on its legitimate interests as the legal ground for processing.

If a data subject would like to access any of these rights they should write to Managing Director, Matrix Networks Limited, 6500 Daresbury Park, Warrington, WA4 4GE.

If a data subject believes that the Company has not complied with their data protection rights, they have the right to complain to the Information Commissioner.

Individual Subject Access

Upon receiving a subject access request, the Company will first ensure that the individual requesting information has a legal right to see this information and will validate the individual's identity.

The Company will gather any manual or electronically held information (including emails) and will identify any information provided by a third party or which identifies a third party. If information is identified which relates to third parties, the Company will write to them asking whether there is any reason why this should not be disclosed. The Company will not supply information unless the other party has agreed for us to do so or it is reasonable to do so without their consent.

The Company will have one month (from when we have received all the information necessary to identify the individual and to identify the information requested) to provide the Data Subject with the information or to provide an explanation as to why this information cannot be provided. The Company may extend the time to respond to a request by a further two months where the request is complex or a number of requests have been received from an individual. In these circumstances the Company will inform the individual without undue delay and within one month of the request being received, explaining why the extension is necessary.

All Subject Access Requests should be made in writing to the Managing Director, Matrix Networks Limited, 6500 Daresbury Park, Warrington, WA4 4GE.

Procedures

The main practical concern is that any data held on a laptop or portable storage such as USB sticks must be securely protected with a password or encryption.

Outlook files must be placed in the encrypted area, to protect sensitive emails from unauthorised access.

Never leave a laptop or portable storage medium in any public place. In particular, do not leave in an unattended car or at a public place. Even if it contains no personal data, other elements such as emails can contain information that is commercially sensitive, and even though it should all be encrypted, it is still a loss of data that could have to be reported.

During a period of annual leave, sickness or unauthorised absence, individual access may be restricted to the Company's systems.

Any breach of these procedures could jeopardise both the company and the client companies. As such it will be treated as the most serious misconduct with corresponding disciplinary action.

Data Breaches

Any data breach should be reported to the Managing Director immediately.

The Company will investigate any potential data breach and, where a breach is found, will report this information to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach.

Where it is found that a breach is likely to result in a risk of adversely affecting individuals' rights and freedoms, the Company must also inform those individuals without undue delay. Where possible, the Company will take any necessary remedial action to limit the consequences of any data breach.

The Company will keep records of all data breaches.

Right to be Forgotten

Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

Individuals can request erasure of their data verbally or in writing. Wherever possible, the Company would ask that requests are made in writing to Managing Director, Matrix Networks Limited, 6500 Daresbury Park, Warrington, WA4 4GE.

The Company will respond to requests within one month of receipt. The Company will not charge a fee unless it feels the request is manifestly unfounded or excessive, in which case the Company may request a reasonable fee.

The Company may extend the time to respond to a request by a further two months where the request is complex or a number of requests have been received from an individual. In these circumstances the Company will inform the individual without undue delay and within one month of the request being received.

The policy itself is subject to annual review.

<End of document>

Reviewed by:	SHEQ Manager	Approved by:	Managing Director
Signature:		Signature: