Data Protection Policy

Section Twenty Five

Policy Statement

This policy sets out our commitment to achieving high standards in Data Protection.

Effective Data Protection is vital to ensure that we receive, manage, and retain data in accordance with our role as an effective Data Controller with the Information Commissioners Office for GDPR (Ref No Z1951458).

Our policy dictates the standardised use, monitoring and management of data and can be used to provide proof in the event of a statutory data protection inspection/s.

We will never distribute and/or share private data without the owner's permission.

Applicable Regulations

We have a legal obligation to manage data in accordance with:

- The Data Protection Act 2018
- The General Data Protection Regulation (GDPR) 2018
- The Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations 2003

We have a legal obligation to create and maintain a record of what we did, how we did it, who did it and who told us we could do it.

Roles & Responsibilities

We will allocate defined roles and responsibilities to employees who handle data.

We have a responsibility to ensure that all data is professionally managed, and this is under the leadership of our Finance DIrector who is responsible to our Board for ensuring that our Data systems, processes, and procedures are compliant with governing legislation.

Guidance Rules

This sets out our guidance to employees on managing records and what responsibilities we have to our clients and individuals. It also governs our use of data, including:

- How decisions were made and taken
- Advice given or received
- Data that supports the decisions that were made

It also features the user operational standards in regards to:

Processes and Procedures

We issue instructions to employees on:

- How to receive, create and store data
- Only storing and using adequate data as long as it is needed
- Keeping data accurate and up to date
- Returning data to clients at the end of a contract
- File Naming convention
- Data retention and disposal actions
- Never transferring data to others outside of our business

Data Security Measures

Our designated person responsible for data protection compliance is Mark Watson

Data, including personal data, is always kept safe and secure through:

- Our registration Certification No IASME-CEP-004308 under Cyber Essentials
- Performing daily backups via secure cloud-based technology
- Access to data being recorded and encrypted to prevent unauthorised access or the introduction of any virus, trojan, malware, or other harmful or malicious software onto our clients' computer systems or software
- Providing a 'Data Wipe' certificate for all data disposal
- Use of technologies and software to prevent Denial-of-Service (DoS) attacks
- Operating role-based security controls with user access permissions limited to appropriate role information
- Data operating procedures which include:
    - Our Password Policy which enforces complexity, password lockout and passwords being changed every 90 days
    - All PCs and handheld devices have automatic time outs and are then locked
    - Screens are protected so that another person cannot view the information when standing or sitting to the side of the user

Data Loss and/or Breach – We will report any relevant events to clients within 24 hours.

Employee Training

We train our employees in our Academy on the processes and procedures for using data, and this includes Induction Training, 6 monthly Core Training and Refresher Training.

Compliance Monitoring

Ongoing monitoring of compliance with this policy and supporting standards will be undertaken on a regular basis by our Data Management Consultants Datcom and any changes are recommended to our Board.

Policy Reviews

This policy will be reviewed annually or at a point where a significant change occurs.

Version No: 3
Issued by: Neil Sanderson – Managing Director