BUFFYROWE.COM GDPR POLICY

My Nutritional Therapy business needs to gather and use certain information about individuals. This policy describes how this personal data will be collected, handled and stored to comply with the UK General Data Protection Regulation.

My Nutritional Therapy Business is committed to a policy of protecting the rights and privacy of clients in accordance with UK General Data Protection Regulation.

My Nutritional Therapy Business commits to:
* Comply with both the law and good practice
* Respect individuals' rights
* Be open and honest with individuals whose data is held
* Register our details with the ICO (Information Commissioner's Office

My Nutritional Therapy Business my hold data for the following purposes:
* Provision of direct healthcare
* Case histories

There are six data protection principles that are core to the UK General Data Protection Regulation. My Nutritional Therapy Business will make every possible effort to comply with these principles and at all times in our information -handling practices. The principles are:
1. Lawful, fair and transparent - data collection must be fair, for a legal purpose and I must be open and transparent as to how the data will be used.
2. Limited for its purpose - Data can only be collected for a specific purpose
3. Data minimisation - Any data collected must be necessary and not excessive for its purpose
4. Accurate - the date I hold must be accurate and kept up to date
5. Retention - I cannot store data for longer than necessary
6. Integrity and Confidentiality - The data I hold must be kept safe and secure

Risks:
The main risks are in two key areas:
* information about individuals getting into the wrong hands through poor security or inappropriate disclosure of information
* individuals being harmed through data being inaccurate or insufficient

Responsibilities:
My Nutritional Therapy Business is the data controller for all personal data held by me and is responsible for:
* Analysing and documenting the type of personal data we hold
* Checking procedures to ensure they cover all he rights of the individual
* Identifying the lawful basis for processing data
* Ensuring consent procedures are lawful
* Implementing and reviewing procedures to detect, report and investigate personal data breaches
* Storing data in sae and secure ways
* Assessing the risk that could be posed to individual rights and freedoms should data be compromised

Data Recording, Security and Storage:
My Nutritional Therapy Business will ensure that any personal data I process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. I will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

My Nutritional Therapy Business will keep personal data secure against loss or misuse.

Storing data securely:
* In cases when data is stored on printed paper, it will be kept in a secure place where unauthorised personnel cannot access it.
* Printed data will be shredded when it is no longer needed
* Data stored on a computer will be protected by strong passwords that are changed regularly.
* Data stored on memory sticks will be encrypted or password protected and locked away securely when they are not being used.
* Cloud services used to store personal data will be assessed for compliance with UK GDPR principles.
* Servers containing personal data must be kept in a secure location, away from general office space
* Data will be regularly backed up
* All servers containing sensitive data must be protected by security software
* All possible technical measures will be put in place to keep data secure

My Nutritional Therapy Business will retain personal data for no longer than is necessary. This shall be in accordance with the guidelines for our professional association, BANT

Accountability and Transparency:
My Nutritional Therapy Business will ensure accountability and transparency in all its use of personal data. I will keep written up to date records of all the data processing activities that I do and ensure that they comply with each of the UK GDPR principles
I will regularly review my data processing activities and implement measures to ensure privacy by design including data minimisation, pseudonymisation, transparency and continuously improving security and enhanced privacy measures.

Consent:
My Nutritional Therapy Business will ensure that consents are specific, informed and plain English such that individuals clearly understand why their information will be collected, who it will be shared with and the possible consequences of them agreeing or refusing the proposed use of the data.
Consents will be granular to provide choice as to which data will be collected and for what purpose.
I will seek explicit consent wherever possible.
I will maintain an audit trail of consent by documenting details of consent received including who consented, when, how, what if and when they withdraw consent.
I will regularly review consents and seek to refresh them regularly or if anything changes.

Direct Marketing:
My Nutritional Therapy Business will seek explicit consent for direct marketing. I will provide a simple way to opt out of marketing messages and be able to respond to any complaints.

Subject Access Requests:
An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice
My Nutritional Therapy Business will provide an individual with a copy of the information requested, free of charge. This will occur within one month of receipt.
I can refuse to respond to certain requests and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, I can request the individual specify the information they are requesting.
Once a subject access request has been made, I will not change or amend any of the data that has been requested. Doing so is a criminal offence.

Data Portability Requests:
I will provide the data requested in a structured, commonly used and machine readable format. This would normally be a PDF file, although other formats are acceptable. We must provide this

data either to the individual who has requested it, or to the data controller they have requested it be sent to within one month.
I will not transfer personal data abroad without express consent.

Third Parties:
As a data processor I will have the written contracts in place with any third-party data controllers that are used. The contract will contain specific clauses which set out my and their liabilities, obligations and responsibilities.
I acknowledge my responsibilities as a data processor under UK GDPR and we will protect and respect the rights of data subjects.

Breaches:
Any breach of this policy or of data protection laws will be reported as soon as practically possible. This means as soon as I become aware of a breach.

My Nutritional Therapy Business has a legal obligation to report any data breaches to UK Supervisory Authority which is the Information Commissioners Office within 72 hours.