Introduction

Katherine Geddes needs to gather and use certain information about individuals. These can include, customers, suppliers, business contracts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the company’s data protection standards – and to comply with the law.

Data protection law

The Data Protection Act 1998 describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. This law is being up dated by the GDPR which comes into effect on the 25th of May 2018. The Data Protection principles include that data must be;

• Be obtained only for specific, lawful purposes: Katherine Geddes is using ‘CONSENT’ and ‘SPECIAL - HEALTH’

• Be adequate, relevant and not excessive

• Be accurate and kept up to date

• Not be held for any longer than necessary

• Processed in accordance with the rights of data subjects

• Be protected in appropriate ways.

People, risks and responsibilities

Policy Scope

The policy applies to:

• Katherine Geddes and anyone who she subcontracts such as a cover therapist or yoga teacher.

• All contractors, suppliers and other people working on behalf of Katherine Geddes

It applies to all data that they/ she holds relating to identifiable individuals. This can

include (but is not a comprehensive list):

• Names of individuals

• Postal addresses

• Email addresses

• Telephone numbers

• Health information…plus any other information relating to individuals

Data protection risks

Data security risks, include:

• Breaches of confidentiality. For instance, information being given out inappropriately.

• Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them, within the scope of the law.

• Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Katherine Geddes has some responsibility for ensuring

data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that it is handled and processed in

line with this policy and data protection principles.

• data protection procedures and related policies will be reviewed as required. Katherine Geddes will arrange data protection training and advice for herself as required.

– Evaluating any third-party services the company is considering using to store or process data. For instance,

cloud computing services.

— Checking data protection statements attached to communications such as emails and letters are fair.

General staff guidelines

• The only people able to access data covered by this policy should be those who need it for their work.

• Data should not be shared informally.

• Katherine Geddes shall check ICO and CSP for guidelines updates annually.

• All data shall be kept secure, by taking sensible precautions and following the guidelines below.

• In particular, strong passwords must be used and they should never be shared.

• Personal data should not be disclosed to unauthorised people,

• Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

• Katherine Geddes will request help from the CSP or ICO if she is unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored.  When data is stored on paper, it should be kept in a secure place where unauthorised

people cannot see it.  These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

• When not required, the paper or files should be kept in a locked drawer or filing

cabinet.

• Katherine Geddes should make sure paper and printouts are not left where

unauthorised people could see them, like on a printer.

• Data printouts should be shredded and disposed of securely when no longer

required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

• Data should be protected by strong passwords that are changed regularly and

never shared.

• If data is stored on removable media (like CD or DVD), these should be kept l

locked away securely when not being used.

• Data should only be stored on encrypted computer and external hard drive, never on the cloud. Data should be backed up frequently.

Data use

Personal data is of no value unless the business can make use of it. However, it is when

personal data is accessed and used that it can be at the greater risk of loss, corruption or theft:

• When working with personal data, I should ensure the screens of my computer is always locked when left unattended.

• Personal data should not be shared informally.

Data accuracy

The law requires Katherine Geddes to take reasonable steps to ensure data is kept accurate and up to date.  The more important it is that the personal data is accurate, the greater the effort should put into ensuring its accuracy.  It is the responsibility of all who work with data to take reasonable steps to ensure it is

kept as accurate and up to date as possible.

• Data will be held in as few places as necessary.

• Katherine should take every opportunity to ensure data is updated.

For instance, by confirming a customers detail’s when they call.

• Data should be updated as inaccuracies are discovered. For instance, if a

customer can no longer be reached on their stored telephone number, it should be

removed from the database.

Subject access requests (SAR)

All individuals who are the subject of personal data held by Katherine Geddes are entitled to:

• Ask what information the she holds of them and why.

• Ask how to gain access to it.

• Be informed how to keep it up to date.

• Be informed how the company is meeting its data protection obligations.

• If an individual contacts the company requesting this information, this is called a

subject access request.Subject access requests from individuals should be made by in writing to Katherine Geddes.Individuals will be charged £10 per subject access request.

Subject access request – Health Records

A ‘health record’ is a record which:

• Consists of information relating to the physical or mental health or condition of

any individual; and

• Has been made by or on behalf of a health professional in connection with the

care of that individual.

‘Heath professionals’ include registered medical practitioners, dentists and nurses and clinical psychologists. The Data Protection Act provides a full list of the types of professionals that fall within the definition (see section 69 of the Act).

Information that forms part of a health record about a living individual is the personal data of the individual it relates to, regardless of the form in which it is held. This means that a subject access request (SAR) can be made for health records in manual form, e.g. paper or in GP’s  medical notes wallets, as well as for health records kept electronically.

Katherine Geddes may charge a maximum fee of between £10 – £50. The precise amount of the maximum fee depends on how the health records are held.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without consent of the data subject.

Under these circumstances, Katherine Geddes will disclose requested data once the  the request is deemed to be legitimate, seeking assistance from ICO and CSP and legal counsel where necessary.

To these ends, Katherine Geddes has a privacy statement, setting out how data relating to individuals is used by the company.

[A hard copy is available on request.]

Right of removal;

|  |  |
| --- | --- |
| Hospital Records |  |
| Children and Young People | Retain until the patient’s 25th birthday or 26th if young person was 17 at conclusion of treatment, or 8 years after death. |
| Mentally disordered persons within the meaning of the Mental Health Act | 20 years after the date of last contact between the patient/client/service user and any health/care professional employed by the mental health provider, or 8 years after the death of the patient/client/service user if sooner |
| All other hospital records ( other than non-specified secondary care records) | 8 years after the conclusion of treatment or death |
|  |  |

Katherine Geddes will comply with current legislation regarding keeping relevant data for accountancy purposes for up to 7 years after they are needed and health information as below to comply with law.

When the records are no longer required I will destroy them by shredding and burning them.

Rights of Clients

All clients will have the right to request a copy of their health records. The needs to be put in writing and the cost of photocopying the records will need to be covered by the requesting client. If there is information in the data that could be deemed harmful to them (ie something a parent said about the child which was relevant at the time). A conversation with my professional body and ICO regarding redacting this information will be had before handing over copies.

When a young person reaches the age of 13, I will discuss the data I have on them and explain to them how long and why I need to keep it. If they request that I destroy it I will refer them to the relevant legislation at the time.

If there is a breach of data. I will inform the client that is directly involved and discuss with them what the breach was and check what they would like me to do. Including informing of relevant authorities including professional body and ICO.