ACCESSIBILITY IN THERAPY
A Needs-Informed Vision for Mental Health

GDPR and Data Processing Policy and Procedure

This policy sets out Accessibility in Therapy CIC (AiT)'s commitment to ensuring that we process any personal data, including special category personal data, in compliance with data protection law. AiT is committed to ensuring that good data protection practices are imbedded in the culture of our organisation.

Scope

This policy applies to all personal data processed by AiT and is part of the organisation's approach to compliance with data protection law. All staff and volunteers are expected to comply with this policy and failure to comply may lead to disciplinary action.

Data protection principles

AiT complies with the data protection principles set out below.

• Personal data is processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
• Personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')
• Personal data is all adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
• Personal data is all accurate and, where necessary, kept up to date. Reasonable steps will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
• Personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation')
• Personal data is processed in a manner that ensures appropriate security of it, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

AiT will:

• facilitate any request from a data subject who wishes to exercise their rights under data protection law as appropriate, always communicating in a concise, transparent, intelligible and easily accessible form and without undue delay
• ensure that the legal basis for processing personal data is identified in advance and that all processing complies with the law
• not do anything with personal data that would not be expected given the content of this policy and the fair processing or privacy notice
• ensure that appropriate privacy notices are in place advising staff and others how and why their

data is being processed, and, in particular, advising data subjects of their rights
• only collect and process the personal data that it needs for purposes it has identified in advance
• ensure that, as far as possible, the personal data it holds is accurate, or a system is in place for ensuring that it is kept up to date as far as possible
• only hold on to personal data for as long as it is needed, after which time AiT will securely erase or delete the personal data – AiT's data retention policy sets out the appropriate period of time
• ensure that appropriate security measures are in place to ensure that personal data can only be accessed by those who need to access it and that it is held and transferred securely

AiT will ensure that all staff who handle personal data on its behalf are aware of their responsibilities under this policy and other relevant data protection and information security policies, and that they are adequately trained and supervised.

Breaching this policy may result in disciplinary action for misconduct, including dismissal. Obtaining (including accessing) or disclosing personal data in breach of AiT's data protection policies may also be a criminal offence.

Rights under the GDPR

The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

Policy
We will provide individuals with information including: our purposes for processing their personal data, our data retention and destruction policy for that personal data, and who it will be shared with.

Procedure
AiT's data policy is visible and accessible through our website. Any forms or data requests explain their purpose, and that service users can choose to opt out at any time.

Subject access

The right to request information about how personal data is being processed, including whether personal data is being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

• the purpose of the processing
• the categories of personal data
• the recipients to whom data has been disclosed or which will be disclosed
• the retention period
• the right to lodge a complaint with the Information Commissioner's Office
• the source of the information if not collected direct from the subject, and
• the existence of any automated decision making (Not applicable at AiT)

Policy
We will respond to a verified enquiry within one month of receiving the response. The procedure is laid out below.

The right to rectification

The GDPR includes a right for individuals to have inaccurate personal data rectified and incomplete personal data completed.

Policy
If a subject contacts AiT at any time and wants their details amended or changed, providing they can confirm that they are the subject in question, we will amend their records accordingly.

Procedure
For written requests we receive we will note where the request came from in our communications on our database, and update details accordingly.

For verbal communications we will again make a note on the communications section of our website, and update details accordingly. If we have doubts as to the identity of the person making the request we will first ask them for identification in writing.

We will action all requests for rectification within one month of receiving the request, excepting where additional identification is required, which we will request, where necessary, as soon as is practically possible.

The right to erasure

The right to have data erased and to have confirmation of erasure, but only :

• the data is no longer necessary in relation to the purpose for which it was collected, or
• where consent is withdrawn, or
• where there is no legal basis for the processing, or
• there is a legal obligation to delete data

Policy
AiT will erase any personal data when it is no longer necessary, if the subject requests an erasure, or in other cases in which it is appropriate

Procedure
If someone objects to our processing their data, or withdraws their consent to hear from us, we will action this request within a month. We will then mark them as dormant and destroy their records, following our data retention and destruction policy.

Restriction of processing

The right to restrict the use of personal data to specific or no processing actions.

Policy
If an individual contacts us wishing to restrict the use of their data, we will make every effort to comply with their wishes.

Procedure
We will mark the subject's record as 'Restricted', meaning that every user will see this warning and will neither amend nor change the subject's details. We will respond to requests both verbally and in writing, providing that we are satisfied that the subject is the subject in question. We will ask for additional identification if we feel additional verification is necessary. We will respond to a request to restrict processing within one month of receiving the request.

The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

Policy

AiT will provide verified subjects with their personal data when requested, including transferring the data to another organisation.

Procedure

If a subject contacts us and asks us to transfer data on their behalf to another organisation we will do so free of charge. Firstly, we will need them to verify their identity, to ensure that it is only their details we are releasing. We will ask them to confirm for us what details they wish to be released. We will then populate a CSV file and make it available to the subject within one month. If the subject requests it, we will transfer the data directly to another organisation on their behalf. This will only be in a CSV format. If the subject requests data about an individual other than themselves, we will need permission and to confirm the identity of all individuals concerned.

The right to object to processing

The right to object to the processing of personal data relying on the legitimate interests processing condition. This is unless AiT can demonstrate compelling legitimate grounds for the processing which override the interests of the data.

Policy

If an individual objects to our processing their data, we will stop processing their data immediately. This is clearly outlined at all points of data collection.

Procedure

If a subject requests we stop processing their personal data, we will respond and comply immediately. All of their details will be marked as no correspondence as soon as possible, and will be destroyed in due course according to our data retention and destruction policy.

AiT does not carry out automated decision making including profiling.

Special category personal data

This includes personal data revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic or biometric data for the purpose of uniquely identifying a natural person
- an individual's health
- a natural person's sex life or sexual orientation
- criminal convictions or offences

AiT processes special category data of clients and third parties as is necessary to provide support and information services.

AiT processes special category data of employees and volunteers as is necessary to comply with employment and social security law. This policy sets out the safeguards we believe are appropriate to ensure that we comply with the data protection principles set out above. AiT also has a data retention policy which sets out how long special category data will be retained.

Data processing, retention and destruction policy and procedure

Article 5 of the GDPR states that data may be kept "no longer than is necessary for the purposes for which the personal data are processed". The key focus of the GDPR is that data is used only for the purposes intended, and not kept longer than necessary.

In accordance with our legal bases for processing data, we will continue to process service user and supporter data under 'Legitimate interests' – to provide these individuals with the service information they expect.

This will include data for attendees at events.

All data subjects who have given marketing information consent or have an identified legitimate interest will be kept as 'active' records, and communicated with on an ongoing basis, as per their personal communication preferences.

When a data subject contacts us and opts out of all communications with us, this will be actioned within one month. This record will be marked as 'dormant' and will no longer be communicated with. The record will be kept on our secure database for a period of six months, then be deleted from our systems. The organisation will carry out data culls of these records once per quarter.

Employee and volunteer data will be retained for six years after the individual's departure from the organisation. This information can and will be presented to HMRC upon request.

Data breaches

All breaches should be reported to the Data Protection Officer (Founding Director).

Under the GDPR, organisations have a duty to report all serious data breaches to the relevant authority within 72 hours of the breach, where possible.

We must also inform the subjects affected, if there is a risk of their rights and freedoms being affected.

We must have robust detection, investigation and reporting procedures in place, and keep a record of any breaches.

Policy

We hold and process a large amount of personal data, a valuable asset that needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidental or deliberate) to avoid a data protection breach that could compromise security. Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs.

We are obliged under the GDPR to have in place a framework designed to ensure the security of all personal data, including clear lines of responsibility and reporting.

This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the organisation.

This policy relates to all data held by the organisation, regardless of format.

The policy applies to all staff and volunteers who access, process, and manage data on behalf of the organisation, including temporary workers and contractors.

For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

An incident is an event or action which may compromise the confidentiality, integrity, or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the organisation's information assets and/or reputation.

An incident includes but is not restricted to the following:

• Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)
• Equipment theft or failure
• Unauthorised use of, access to, or modification of data or information systems
• Attempts (failed or successful) to gain unauthorised access to information or IT systems
• Unauthorised disclosure of sensitive / confidential data
• Website alterations
• Hacking attack
• Human error
• 'Blagging' offences where information is obtained by deceiving the organisation who holds it

Procedure

Any individual who accesses, uses, or manages the organisation's information is responsible for reporting a data breach and information security incidents immediately to the Data Protection Officer (Founding Director) via email – follow up by phone. Please note it should still be reported in this manner even if discovered outside normal working hours, as it may require reporting to ICO within 72 hours.

The report must include full and accurate details of the incident, including:

- when the breach occurred (dates and times)
- who is reporting it
- if the data relates to people
- the nature of the information
- how many individuals are involved

A data breach reporting form (below) should be completed as part of the process and must be securely stored for future reference.

The DPO, alongside other relevant staff (depending on the nature of the incident) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach. An initial assessment should be carried out by the DPO and the relevant team members to establish how severe the breach is, and who should investigate further, depending on the nature of the breach and the information that has been breached. Whoever investigates the breach must report back to the (DPO) Chief Executive. The person investigating the breach must establish if there is anything that can be done to recover any losses and limit the damage, and who needs to be notified of the breach, including the police if appropriate. They will then determine a suitable course of action to be taken to resolve the incident as quickly as possible. The person investigating the breach will need to consider:

- The type of data involved
- Whether any of the data is special category data
- If the data is protected or encrypted in any way
- If the data has been accidentally lost, or deliberately stolen
- Whether the data could be used for any illegal purposes
- Whose data has been breached, and how many individuals are included, and the potential effects on them

The DPO will then determine who needs to be notified of the breach. Each case will be considered on an individual basis and the DPO will determine whether the breach would need to be reported to the ICO. The DPO will then consider if the individuals affected need to be notified directly, and if doing so would prevent unlawful use of their personal data. Guidance on notifying the ICO can be found on the ICO website and via their helpline. The DPO must also consider notifying legal authorities or bank or credit card companies, and making a public press release available where necessary. Once the investigation is over, AiT will undertake a review of the relevant policies and procedures to see if any changes can be made to better protect against future breaches and assess the effectiveness of the investigation and responses.

Subject Access Request procedure

We have the following process in place following a SAR:

1) Set a timetable.

a. Upon receiving a SAR, document when it was received and the date by which the request must be completed. We will aim to address all SAR within one month.

b. Establish the subject's identity. The person making the request must establish to the satisfaction of the organisation that they are requesting their own information. Requests for information on other parties will be denied.

c. Establish what information the subject wants. If it is unclear what the subject wants to know we will ask them promptly for additional information so that we can comply with their request. If we are unsure, we will provide all information, subject to exemptions.

d. Confirm no fees will be charged. As a small charitable organisation AiT will not charge a fee for a SAR, unless the request is so unreasonable as to justify a charge. If the subject wishes to make a donation to our work, we will accept this.

e. Confirm we have the information requested. If AiT does not have the information requested by the subject, inform them of this. If we do have it prepare it for transfer.

f. Confirm that no changes can be made to the information. The format of the information may be changed, for example exporting from our database into a PDF for the subject to view, but no changes to the information itself can or will be made. The only exception to this is if the subject wants information about other people. We cannot release information about other people without their express consent. Without such consent the identities of other persons will be redacted.

g. Confirm how the subject wishes to receive their information. We can send information both electronically and in hard copy by post, at the requester's preference.

h. Confirm what data is supplied. AiT will make every effort to disclose what personal information we hold about the subject, including biographic details, their history with the organisation and a history of any financial transactions. We will also supply details of any processing that their data undergoes and the reasons for this. If we hold no data on the subject, we will confirm this.

i. Provide a copy of the data we hold. Depending on the subject's choice this will be sent electronically as a PDF document or a hard copy will be posted, in clear and easy to understand language. We will not send fax communications for security reasons.

j. We may refuse a SAR, and when we do, this will be discussed with the Data Protection Officer and clearly documented to the subject.

Data Security

A key requirement under the data protection laws is that AiT consider where data is held, including laptops, memory sticks, and our information systems and suppliers.

Policy

All reasonable steps will be taken to protect staff, volunteer, supporter, and service user data . At least every two years we will review our IT systems. Including our firewalls, website security, and key systems access.

Procedures

Devices

Staff use personal devices for their work. Staff should ensure that these devices are not used by other individuals. If other individuals do use staff's personal devices, any access to personal or sensitive data relating to AiT or anyone involved with the organisation should be through a separate, password-protected profile.

Staff should only access email or files when using a secure Wi-Fi or 3/4G connection.

Passwords

Personal passwords for IT systems should not be shared and should be changed at least every quarter.

Email access

Our emails are accessed within the office 365 suite. If these are accessed on personal devices files should not be downloaded. The personal device should have a strong password, thumb print or facial recognition to access. If lost, the email password should be changed immediately.

File Saving

All files containing personal data should be saved only in the Office 365 suite or within the relevant CRM. No files should be saved to personal hard drives of computers, laptops or memory sticks.

File sharing

Great care should be taken if personal or sensitive data is shared outside of AiT. This should never be done by memory stick or CD. Need to transfer the data should always be carefully considered, and line manager agreement sought wherever relevant. Data transferred should always be password protected and the password shared by an alternative media.

Travel

Carrying personal or sensitive data should be minimised. If data has to be carried a short risk assessment should be undertaken to ensure that risk of data loss is minimised during travel.