



Confidentiality and General Data Protection Regulations (GDPR) Policy

ICO

Mindsong is registered with ICO – the Information Commissioner’s Office. Registration Number ZA795787. This registration is reviewed in line with ICO recommendations annually by the Chief Executive and Trustees and renewed for the 13 Oct each year.

Introduction

Mindsong recognises that anyone who works with us in a voluntary or professional capacity, who supports us or who receives any service from us, has the right to expect that any information we hold about them will be held securely, confidentially and in accordance with the data protection act 1998.

This sets out Mindsong’s policy and procedure to protect and safeguard any person-identifiable information that is gathered, created or disclosed.

Person-identifiable information is anything that contains the means to identify a person such as name, address, postcode, date of birth.

Under the Data Protection Act we must:

- Use personal information fairly and lawfully
- Collect only the information necessary for a specific purpose(s)
- Ensure it is relevant, accurate and up-to-date
- Only hold as much as we need, and only for as long as we need it
- Allow the subject of the information to see it on request
- Keep it secure

Our data protection & confidentiality contact is: the Chief Executive

Our data protection lead is: Director of Music Therapy who is HCPC & BAMT registered.

Our Trustee Lead is: Helen Owen

Staff Responsibilities and Training

We verbally outline to staff and volunteers their rights, how to exercise this is reinforced in both the staff/volunteer handbook and initial briefing

All members of the Mindsong Team must read and adhere to our Privacy Statement and our Confidentiality and GDPR policy; training will be given where necessary.

All staff, which includes volunteers, should read this policy carefully and raise any questions with the Data Protection lead to ensure they are clear on their responsibilities.

All staff must ensure that participants & clients are given access a copy of the relevant Privacy Statement and explain how they can exercise their rights.

Mindsong will;

- Provide a data protection briefing on induction and training on any aspects relevant to a particular role
- Provide training to all staff collecting or handling data
- Provide core staff training every three years
- Keep up to date on legislation through the Data Protection lead and inform all staff when there are significant updates or changes to legislation
- Include data protection on board agendas

Review of Data Processing and Compliance

Mindsong will carry out a data audit which will be reviewed annually. This covers:

- what personal data we process
- why we process it
- how we have communicated this information to the data subject
- whether this is special category data
- a confirmation that this is the minimum data required to complete the task
- how the data is kept securely
- how long the data is held for
- how the data is checked for accuracy and kept up to date
- any actions required

After each review, relevant staff members will then be briefed as to their responsibilities and the actions needed relating to different data.

In addition to the above, where we are collecting sensitive data, we must meet one or more additional criteria to have a reason to process the data. Those that are relevant to our work include:

- The individual (or their representative) whom the sensitive personal data is about has given explicit consent to the processing
- The processing is necessary so that we can comply with employment law
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals

Data Quality

Mindsong understands the requirement for effective data quality maintenance and annually reviews data monitoring and cleaning. Maintenance involves updating/standardising data and de-duplicating records.

Data quality maintenance checks, overseen by Mindsongs Chief Executive, includes checks on:

- Completeness: Level at which desired data attributes are supplied. Data does not need to be 100% complete
- Accuracy: Randomised checks back against original documents such as assessment forms
- Credibility: Any data obtained from outside Mindsong will be checked to what extent it is relevant and true
- Timeliness (age of data): Extent to which data is adequately updated for a current programme of work
- Consistency: Assessment as to whether various dataset facts match
- Integrity: Assessment of reference validity and accurate joining of various datasets
-

Actions and Compliance

Participation

- ensure participants' data is only processed with their consent
- ensure participants' data is only shared on a need to know basis e.g. medical information with referrer or relevant clinician
- ensure all volunteers and freelance staff are briefed regarding their data protection responsibilities regardless of how short their contract is

Operations

- ensure website privacy policy and cookie policy is clear and compliant and online providers have been audited
- ensure audits, staff training and briefings are carried out
- ensure IT policies are in place and compliant and staff are briefed
- ensure IT software and hardware is audited and offers sufficiently robust security
- ensure procedures are in place for responding to data breaches, subject access requests, data portability and requests for the right to be forgotten and to support staff in responding to such requests

Breaches

In the event of a security breach, the Data Protection lead must be informed immediately.

Depending on the circumstances of the breach, action will include:

- completing an incident report
- taking action to address the cause of the breach
- taking action to minimise the damage that may be caused by this data not being kept securely
- possible disciplinary action

If the breach is likely to result in a risk to people's rights and freedoms, for example discrimination, damage to reputation or financial loss, it is mandatory to report a personal data breach to the ICO within 72 hours. The Data Protection lead will make this report and also report to the Chair of trustees.

This may then also need to be reported to the Charities Commission as a serious incident that has been reported to a third party regulator.

If a member of staff realises that they have been processing data in a way not compatible with the data audit or with the way in which it was originally collected they must also inform the Data Protection lead as soon as possible so a plan of action can be agreed.

1. Security

All Mindsong professionals work from their own homes. We must therefore take all realistic precautions to safeguard person-identifiable information.

- 1.1 All paid professionals must ensure that any electronic equipment (including laptops, tablets and mobile phones) used to store records or data is secured with a strong password or similar device. Passwords must not be shared and if written down, stored securely.
- 1.2 Where records or data are stored on a shared device, all documents must be stored in the nominated secure file sharing app.
- 1.3 Records or confidential reports should not be stored on removable media such as flash drives or portable hard drives.
- 1.4 Sharing of confidential reports or data within the organisation, when not shared in person, should be done via a secure file sharing app.

- 1.5 All reports should be anonymised (or pseudonymised where requested for certain services) except when sharing with the client, care home or other relevant professional involved.
- 1.6 Sharing with appropriate external organisations or individuals must be by registered post with the client's consent.
- 1.7 Any personal information held on paid professionals will be held securely at the administration office.

2. Personal Data – Our Clients

2.1 Music Therapy is a confidential service whereby music therapists are bound by HCPC legislation to keep client details and what happens during therapy confidential. There are a number of exceptions to this rule:

- The therapist may talk about the therapy and client within the bounds of confidential supervision
- The therapist may share information about the therapy and client for reporting and presentation purposes *with the client's consent**
- The therapist may share relevant information, where appropriate, with colleagues involved in the care, treatment or other services provided to a client
- The therapist may also share information if it is in the client's best interests; or – in the public interest, such as if it is necessary to protect public safety or prevent harm to other people

2.2 Clinical Notes

Music therapists are required by HCPC regulations to keep clinical notes. These must comply with the BAMT guidelines for writing, transporting and storing clinical notes, which can be found on their website under 'Guidance Documents' www.bamt.org, in the relevant file in the nominated file sharing app, or from Director of Music Therapy, Maggie Grady maggie.grady@btinternet.com

2.3 Audio / Visual Recordings

Recordings of therapy sessions may be made for supervision purposes, with the client's consent.*

Any recordings made must be stored securely on a password protected device or locked in a filing cabinet. Further consent is necessary when using any recordings in presentations or reporting. No audio / visual records may be uploaded to the internet.

Mindsong asks all their therapists to follow the BAMT guidelines for the use of audio and video records, which can be found on their website under 'Guidance Documents' www.bamt.org in the relevant file in the nominated file sharing app, or from Director of Music Therapy, Maggie Grady maggie.grady@btinternet.com

2.4 Photographs

Sometimes photographs are taken to illustrate our website or presentations. These will only be taken and used with consent from the persons involved.* Photographs will be stored securely in the nominated file sharing app.

2.5 Sharing Information

Sometimes it is necessary to share sensitive information with wider contacts, for example, Community Dementia Nurses or GPs. Where possible, this will be done by meeting face to face or over the phone, otherwise by registered post.

When sharing confidential information face to face and in other than a dedicated space, it is important that you cannot be overheard.

2.6 Confidentiality Awareness for Volunteers

Our volunteers work in care homes, day centres and at times in private homes, with vulnerable adults. We expect all volunteers to respect the privacy of everyone they work with by not discussing individuals outside of the work environment, except during training or supervision.

3. Data collection and use

3.1 Volunteers

- All email or postal addresses supplied by our volunteers will be used for internal communication only
- All databases are held on secure online software and are not shared with anyone except Mindsong employees.
- Any information held on retired volunteers will be deleted
- Any and all images of volunteers used in printed material, or online, for public view are used with the permission of the individual involved

3.2 Email databases

- We hold a database of anyone interested in Mindsong and who has requested communications from us. This database is held via a secure online app and is not available to anyone outside of the organisation in any form
- Anyone on the database has the option to unsubscribe at any time

3.3 Participants

- All person identifiable data collected on participants in courses other than music therapy is kept securely
- All data is shared with the commissioning body and delivered securely as requested by the commissioning body

*Where informed consent is not possible special consideration will be given, and consent from relative or carer will be sought.

ICO

Mindsong is registered with ICO – the Information Commissioner’s Office.

Registration Number [ZA795787]

This registration is reviewed in line with ICO recommendations annually by the Chief Executive and Trustees and renewed for the 13th October each year.