Taking Part
Confidentiality and Data Protection Policy

Changing Times, Changing Lives

Taking Part is a Charitable Company Limited by Guarantee.
Registered Office: Louise House, Roman Road,
Meole Brace, Shrewsbury, Shropshire SY3 9JN
Registered in England. Reg. No. 4362948, England and Wales, Registered Charities No. 1092033

[1] Revised May 2018

Confidentiality Policy

One of the guiding principles of Advocacy is CONFIDENTIALITY.

General Rules

Taking Part keeps all information received and recorded on clients and/or referrals confidential and secure. All stored information is subject to:

General Data Protection Regulation 2018
Access to Personal Files Act 1987
Access to Medical Report Act 1988 Access to Health Records Act 1990

Therefore, any person using Taking Part's service will be informed that they rights regarding any information which is heldor processed about them.

The duty of confidentiality does not override breaches of the law or situation of extreme risk. Where possible such issues should be reported to the Charity Manager or a senior colleague before action is taken.

Information on Staff, Volunteers and trustees

All information on staff, volunteers and trustees to be stored in locked filing cabinet or on a secure online portal. Any information which may be kept on computer, other than names and addresses, will be protected by the General Data Protection Regulation.

Staff, volunteers and trustees have the following rights regarding information held and processed about them;

- **To know the lawful purpose; contract**

All staff, volunteers and trustees are required to sign a contract of work at the start of their employment and are given copies of this and all Taking Part policies.

- **How we hold and process information and who it will be shared with;**

Access to personnel files is to be open to the member of staff, Charity Manager and Board of Trustees. Recruitment and training records may, from time to time, be requested by Funders or other relevant bodies for inspection. All information to be stored in locked filing cabinet in a locked office. Any information which may be kept on computer will be protected by the General Data Protection regulation. Any staff, volunteer or trustee personal data that is taken away from the office must be transported in a locked case. Any staff, volunteer or trustee date that is stored off premises must be kept in a locked case in locked premises.

A record of all processing of data, whether verbally or through file transfer will be recorded in staff, volunteer or trustee files, and will include the date the recipient of the data and a brief description of data transferred.

- **Data retention periods;**

All staff, volunteers and trustees information will be held for 7 years after termination of contract, in line with Local Authority and other funding bodies requirements.

- **Individual rights under the law;**

the right to be informed;
All staff, volunteers and trustees will be given a copy of relevant policies and informed of rights under GDPR.
the right of access;
All staff, volunteers and trustees will have access to their own file with the exception of references which the referees may request to remain confidential. Any request from staff, volunteer or trustee to access their information, whether verbal or written, will be referred to the Privacy Officer without delay. The Privacy Officer will record the request, assess the nature of the request and make a decision as to whether the request will be granted within one month. The Privacy Officer will then correspond with the applicant to either organise for the claimant to access their records or explain why this request has been denied. The outcome will also be recorded.
the right to rectification;
All staff, volunteers and trustees have the right to amend any personal information on them which is factually inaccurate.
the right to erasure;
All staff, volunteers and trustees have the right to have their information erased, however, this will impact on Taking Part's ability to support them in their role.
the right to restrict processing;
All staff, volunteers and trustees have the right to restrict how Taking Part process their information, however, this may impact on how Taking Part can support them in their role.
the right to data portability;
Taking Part do not currently process any personal information through automated means.
the right to object:
staff, volunteers and trustees do not have the right to have their data processed as the lawful purpose for this is contract.
the right in relation to automated decision-making and profiling;

staff, volunteers and trustees do not have rights in relation to this as the lawful purpose for processing is contract.

- **Information on Special Category Data**

Taking Part hold and process certain personal information that is sensitive, including race;ethnic origin;politics;religion; trade union membership;genetics; biometrics (where used for ID purposes);health;sex life; sexual orientation. This is held and processed under the lawful purpose of **contract** and processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; - see Data Protection Act Article 9(b).

- **Information on Criminal Offence Data**

Some staff will undergo a DBS check, Taking Part only record when it has been done, not what the outcome is, unless we have had a conversation about the outcome of this check, notes from which will be recorded.
Any information relating to Criminal Offence Data will be held and processed under the lawful purpose of **contract.** This is in accordance with Article 6 and 10 of GDPR with the additional safeguards set out in the Bill see DPB clauses 9 and 10, schedule 1.

- **How to complain to ICO**

All staff, volunteers and trustees have the right to complain to the Information Commissioners Office if they have concerns about Taking Part's information right's practises. This can be done online at https://ico.org.uk/make-a-complaint/ or by telephone on 0303 123 1113.

Information on clients

Clients have the following rights regarding information held and processed about them;

- **To know the lawful purpose; consent.**

All clients are asked to sign a consent form at the initial meeting with Taking Part. Clients are given the option to complete this and have choice as to how their information is processed.This consent is reviewed by staff member throughout the case. All clients will be informed of their rights by staff at the initial meeting and be given 'The Role of an Advocate' or Privacy Notice documents, which includes their rights under the GDPR.

If consent from client is not possible following an capacity assessment under the Mental Capacity Act 2004, a third party with the legal right to make decisions on their behalf (eg under a Power of Attorney) can give consent.

- **How we hold and process information and who it will be shared with;**

All information on clients to be stored in locked filing cabinet in a locked office or on a secure online portal in line with the General Data Protection Regulation. Staff members who take client personal data away from the office are required to transport this data in a locked case. Staff members are required to store any client personal data in a locked case in locked premises.
Staff must be free to discuss their individual workload and issues of any nature with the Charity Manager. This is essential for the protection and well-being of all parties.
Lacking capacity following Mental Capacity Act (MCA) decision in line with MCA Guidelines and for referrals that been received where the client lacks capacity to consent will be accepted under working practice of 'non-instructed' advocacy. Staff will work in a multi-disciplinary approach with others and sharing of data will only be on the basis and purpose of this referral. This is as per Advocacy Code of Practice and Non-Instructed Advocacy Policy. The sharing of information will then be done following a 'Best Interest' decision process and where sharing of the information will advance the advocacy process or work involved with at that time.
Where staff are working with clients who have given consent for referrals and through working with clients then reflect on client's capacity to understand information and give consent to data sharing, then staff should discuss with Charity Manager with a view for request of a Mental Capacity Assessment of the client.
If there is a risk to the client of either self-harm or harm to others, staff must disclose that information to the Charity Manager in order to discuss or be advised what action to take and the implementation guidance of Safeguarding Policy.
A record of all processing of data, whether verbally or through file transfer will be recorded in client files, and will include the date the recipient of the data and a brief description of data transferred.

Processing information;
When sending emails about clients, then limited information should be sent to third parties – use of initials or first name is preference. At no time should name, DOB or address be sent in any one email.
If documents need to be shared via email, then they should be password protected whenever possible or sent through secure portals/systems.
When sending documents to third parties, any reference to client and/or family or any identifiable data including reference numbers if part of enquiry/referral should be redacted. This should be done using any suitable means (black marker, labels, re-typing). Once documents have been amended, they should be checked by a 2nd member of staff for completeness before sending onto the third party.

- **Data retention periods;**

All clients' information will be held for 7 years after termination of contract, in line with Local Authority and other funding bodies requirements.

- **Individual rights under the law;**

the right to be informed;

All clients will be informed of their rights by staff at the initial meeting and be given 'The Role of an Advocate' or Privacy Notice documents, which includes their rights under the GDPR.

the right of access;

Client's have the right to access their information.

If information is given by a third party, consent from them needs to be obtained before sharing it with the client.

If staff receive information about the client from other parties and are asked not to share this data with the client, then the staff member will question and challenge this request quoting Valuing People 2001 principle 'Nothing About Us Without'. Only where it is determined that sharing information would be detrimental to the health and well-being of the client would this request be considered. In any such circumstances, staff will advise and/or seek guidance from the Charity Manager.

Any request from a client for access to their information, whether verbal or written, will be referred to the Privacy Officer without delay. The Privacy Officer will record the request, assess the nature of the request and make a decision as to whether the request will be granted within one month. The Privacy Officer will then correspond with the applicant to either organise for the claimant to access their records or explain why this request has been denied. The outcome will also be recorded.

the right to rectification;

All clients have the right to amend any personal information on them which is factually inaccurate.

the right to erasure;

All clients have the right to have their information erased, however, this will impact on Taking Part's ability to support them.

the right to restrict processing;

All client's have the right to restrict how Taking Part process their information. Consent will be gained at the initial meeting through the consent form. Ongoing consent will be gained by staff and recorded in case notes before any data is shared with third parties.

the right to data portability;

Taking Part do not currently process any personal information data through automated means.

the right to object;
All clients have the right to object to their data being processed for marketing purposes. Clients can also object if the processing is for:

- a task carried out in the public interest;
- the exercise of official authority vested in you; or
- your legitimate interests (or those of a third party).

In these circumstances the right to object is not absolute.

If a client raises an objection, whether verbal or written, it will be referred to the Privacy Officer without delay. The Privacy Officer will record the objection, assess the nature of the objection and make a decision as to whether the objection will be upheld within one month. The Privacy Officer will then correspond with the client to discuss this decision. If the objection is not granted, the Privacy Officer will also inform the client of their right to complain to the ICO or seek to have their right enforced through judicial remedy. The outcome will also be recorded.

the right related to automated decision-making including profiling;

Taking Part do not use automated programmes to process data.

- **Information on Special Category Data**

Taking Part hold and process certain personal information that is sensitive, including race;ethnic origin;politics;religion; trade union membership;genetics; biometrics (where used for ID purposes);health;sex life; sexual orientation. This is held and processed under the lawful purpose of **consent** and the client has given **explicit** consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; Paragraph 1 can be lifted under Data Protection Act under Article 9(h) - (a) by or under the responsibility of a health professional or a social work professional, or (b) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

- **Information on Criminal Offence Data**

Taking Part do not hold or process information relating to Criminal Offence Data unless it is necessary to the work done with the client.
Any information relating to Criminal Offence Data will be held and processed under the lawful purpose of **consent.** This is in accordance with Article 6 and 10 of GDPR with the additional safeguards set out in the Bill see DPB clauses 9 and 10, schedule 1.

- **How to complain to ICO**

All clients have the right to complain to the Information Commissioners Office if they have concerns about Taking Part's information right's practises. Staff inform all clients of this at the initial meeting, it is also stated on 'The Role of Advocate' and 'Privacy Notice' documents that are given to clients.

Implementation of Policy

All staff upon start of employment and part of the Induction Programme to Taking Part are to familiarise themselves with policy on confidentiality and to adhere to guidance and process.

Breaches of confidentiality

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.
If a data breach has occurred, the Privacy Officer will be informed immediately. The Privacy Officer will undertake an assessment of risk to the individual's rights and freedoms. If a risk to these is identified, the Privacy Officer will should try to contain the breach, assess the potential adverse consequences for individuals and then notify the Information Commissioners Office without delay (within 72 hours). The Privacy Officer will make a record of the breach in the Impact Assessment Log, including;

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If the data breach is likely to result in a high risk to the rights and freedoms of the individual, they must also be notified without delay. The information given to the individual will include;

- the name and contact details of your data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

The Privacy Officer will also investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

Appendix A:

Confidentiality Dos and Don'ts

Dos

• Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with.
• Do clear your desk at the end of each day, keeping all portable records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
• Do switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any length of time.
• Do ensure that you cannot be overheard when discussing confidential matters.
• Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
• Do share only the minimum information necessary.
• Do transfer person-identifiable or confidential information securely when necessary
• Do seek advice if you need to share patient/person-identifiable information without the consent of the client
• Do report any actual or suspected breaches of confidentiality.
• Do participate in induction, training and awareness raising sessions on confidentiality issues.

Don'ts

• Don't share passwords or leave them lying around for others to see.
• Don't share information without the consent of the person to which the information

relates, unless there are statutory grounds to do so.
• Don’t use person-identifiable information unless absolutely necessary, anonymise the information where possible.
• Don’t collect, hold or process more information than you need, and do not keep it for longer than necessary.

Impact Assessment Log Template May 2018

Date	
Event	
Name of Privacy Officer	
Who Involved	
Category of data	
Likely consequences of breach	
Has individual been informed?	
Has ICO been informed?	
Other actions taken	
Date resolved	