Taking Part
Confidentiality 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 2020

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. Any information stored and managed by Taking Part is subject to:

Data Protection Act (2018)
General Data Protection Regulation (2018)
Access to Medical Report Act (1988)
Access to Health Records Act (1990)

Any employee, trustee or volunteer or anyone using Taking Part's service will be informed that they have rights regarding any information which is held, or processed, by Taking Part about them.

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

When Confidentiality can be Breached:

A decision to breach confidentiality must always be taken very seriously. Although information about a member of staff, volunteer, trustee or client must not usually be passed on to a third party without the individual's permission, there are infrequent exceptions where there is evidence that:

- The individual, or someone else, is at risk
- The good name and reputation of Taking Part and the service it provides is at risk
- Disclosure of information is required by law
- A potential conflict of interest is identified or exists

Before a breach of confidentiality is sanctioned, a judgement as to whether there is a serious risk of danger to the individual or others, or to the Taking Part service, has to be made.

This must be done in conjunction with the Privacy Officer unless there is:

- An immediate and urgent risk
- A safeguarding concern about a child or a vulnerable adult

If Taking Part breaches staff, volunteer, trustee or client confidentiality without following

the procedure laid down in this document the incident should be reported to the Privacy Officer as soon as possible for investigation and further action if necessary.

Information on Staff, Volunteers and Trustees

All information on staff, volunteers and trustees is to be stored in a 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 (2018) or GDPR.

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 a copy of this and copies of all Taking Part policies and procedures.

- **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, the Charity Manager and the Board of Trustees. Recruitment and training records may, from time to time, be requested by external funding authorities or organisations or other relevant bodies for inspection. All information is to be stored in a 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 personal data that is stored off site must be kept in a locked case in locked premises.

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

- **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 body 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 procedures and informed of their rights under Data Protection and GDPR legislation.

the right of access;

All staff, volunteers and trustees will have access to their own data file with the exception of references which the referees may request to remain confidential. Any request from a member of staff, a volunteer or a trustee to access their personal 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 of the initial request. The Privacy Officer will then correspond with the applicant to either organise for them to access their records or explain why this request has been denied. The outcome will also be recorded.

If, when considering a request for access to an individual's personal information, the Privacy Officer feels that disclosure of the information at this point in time would cause or escalate that individual's anxiety and stress levels, the decision to withhold that information from the person may be taken. The Privacy Officer will consider whether granting access to the information would cause significant acute distress for the individual and whether the information could be shared in a different way and at a time that would have less impact on the individual. This process will be undertaken, as far as possible, in conjunction with the individual and all details and outcomes of the decision making process will be recorded.

the right to rectification;

All staff, volunteers and trustees have the right to amend any personal information held about 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 processes 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:

All staff, volunteers and trustees do not have the right to object to having their data processed as the lawful purpose for this is contract.

the right in relation to automated decision-making and profiling;

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

- **Information on Special Categories of Personal Data**

Taking Part hold and process certain personal information that is sensitive, including racial or ethnic origin; political opinions; religious or philosophical beliefs; 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; - Data Protection Act (2018)

- **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 DPA (2018) 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 data management and information rights 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 the choice as to how their information is processed. This consent is reviewed by the allocated 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' and any Privacy Notice documents, which includes their rights under the GDPR.
If a third party is needed to help with communication with the client (e.g. community language interpreter, sign language interpreter or family member) consent from the client will be sought, where possible, and recorded on the consent form. If the client is unable to give consent because of language barriers

or other communication needs, then the member of Taking Part staff will do their best to explain that help is required (e.g. through the use of basic Google translator, pictorial aids) before engaging an independent third party to assist. In the first instance, no personal information or data will be shared with the third party, only the communication needs of the client.
Once the third party has been introduced to the client and communication established, Taking Part will seek consent from the individual to allow the third party to act with the Taking Part staff in the case and for information and data relevant to the case to be shared with them. This consent will be recorded in the case notes.
If consent from a client is not possible, following a capacity assessment under the Mental Capacity Act 2004, a third party with the legal right to make decisions on the client's behalf (e.g. under a Lasting Power of Attorney) can give consent for the data to be collected and held.

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

All information on clients is to be stored in locked filing cabinets, 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**

Referrals received where the client lacks capacity to consent will be accepted under the working practice of 'non-instructed' advocacy. Staff will work in a multi-disciplinary approach with others and personal data about the client will only be shared on this 'need to know' basis and for the purpose of this referral. This is as per the Advocacy Code of Practice and Taking Part's Non-Instructed Advocacy Policy. The sharing of information will then be completed following a 'Best Interest' decision process and only where sharing of the information will advance the advocacy process or any work involved with the client at that time. Details of the best interest decision making process will be recorded by the advocate and kept with the client's data file – this record will detail the best interest decision being considered, the individuals involved in the decision making process and the outcome of the process.

If a member of Taking Part staff is working with a client who initially gave consent for the referral and for their personal data to be held and managed by Taking Part but where, based on their experience working with the client, the staff member feels that the client's capacity to understand information and give consent to data sharing is questionable, then the staff member should discuss this with the Charity Manager, with a view to requesting 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 the circumstances for guidance or to be advised what action to take in relation to the implementation of the 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 of the transaction, the recipient of the data and a brief description of data transferred.

- **Processing information;**

When sending emails about clients, then limited information should be disclosed to any third party – the client's identity should be protected through the use of their initials or first name only as a preference. At no time should the client's full name, date of birth or address be sent in any one email.

If documents need to be shared via email, then the document should be password protected whenever possible or sent electronically through a secure portal/system. When sending documents to a third party, any reference to the client and/or family or any identifiable data including reference numbers, if part of the enquiry/referral, should be redacted. Taking Part staff are aware that guidance on redacting reports and case notes is provided by the Information Commissioner's Office (https://ico.org.uk/) The redaction of sensitive data should be done using any suitable means (e.g. using a redacting pen or permanently deleting identifying data in an electronic report rather than using filled blocks of colour over text, where the use of the spacebar could reveal the hidden text). Once documents have been suitably amended, they should be proofread and checked by a 2nd member of staff for completeness before sending onto the third party.

- **Data retention periods;**

All Taking Part client information will be held for 7 years after termination of activities, in line with Local Authority and other funding body requirements.

- **Individual rights under the law;**

the right to be informed;

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

the right of access;

Clients have the right to access their personal data and information.
If information is given by a third party, consent from the third party needs to be obtained before it can be shared 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 the Valuing People 2001 principle 'Nothing About Us Without Us'. 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 of the initial request. The Privacy Officer will then correspond with the applicant to either organise for them to access their records or explain why this request has been denied. The outcome will also be recorded.

If, when considering a request for access to an individual's personal information, the Privacy Officer feels that disclosure of the information at this point in time would cause or escalate that individual's anxiety and stress levels, the decision to withhold that information from the person may be taken. The Privacy Officer will consider whether granting access to the information would cause significant acute distress for the individual and whether the information could be shared in a different way and at a time that would have less impact on the individual. This process will be undertaken, as far as possible, in conjunction with the individual and all details and outcomes of the decision making process will 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 clients 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 data 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 racial or ethnic origin; political opinions; religious or philosophical beliefs; 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 their 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 being 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 DPA 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 as part of the Induction Programme to Taking Part are to familiarise themselves with policy on confidentiality and to adhere to the 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 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 client/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.

Appendix B

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	