PRIVACY POLICY

HT Counselling ("**HTC**") as a service is committed to complying with data protection law and to respecting the privacy rights of individuals. The policy applies to all of our counsellors, trainee's, volunteers and consultants ("**Workers**").

This Data Protection Policy ("**Policy**") sets out our approach to data protection law and the principles that we will apply to our processing of personal data. The aim of this Policy is to ensure that we process personal data in accordance with the law and with the utmost care and respect.

We recognise that you have an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy and to apply and implement its requirements when processing any personal data. ***Please pay special attention to sections 14, 15 and 16 as these set out the practical day to day actions that you must adhere to when working or volunteering for HT Counselling.***

Data protection law is a complex area. This Policy has been designed to ensure that you are aware of the legal requirements imposed on you and on us and to give you practical guidance on how to comply with them. This Policy also sets out the consequences of failing to comply with these legal requirements. However, this Policy is not an exhaustive statement of data protection law nor of our or your responsibilities in relation to data protection.

If at any time you have any queries on this Policy, your responsibilities or any aspect of data protection law, seek advice from Lead Counsellor for HTC ("**LC for HTC**"), Helen Townsend

1. Who is responsible for data protection?

1.1. All our Workers are responsible for data protection, and each person has their role to play to make sure that we are compliant with data protection laws.

1.2. We are not required to appoint a Data Protection Officer (DPO), However we must still ensure that we are compliant.

2. Why do we have a data protection policy?

2.1. We recognise that processing of individuals' personal data in a careful and respectful manner cultivates trusting relationships with those individuals and trust in our service. We believe that such relationships will enable our organisation to work more effectively with and to provide a better service to those individuals.

2.2. This Policy works in conjunction with other policies implemented by HTC from time to time.

3. Status of this Policy and the implications of breach

3.1. Any breaches of this Policy will be viewed very seriously. All Workers must read this Policy carefully and make sure they are familiar with it. Breaching this Policy would see a restriction/termination of any hire contract to any Workers.

3.2. If you do not comply with Data Protection Laws and/or this Policy, then you are encouraged to report this fact immediately to LC for HTC,. This self-reporting will be taken into account in assessing how to deal with any breach, including any non-compliance which may pre-date this Policy coming into force.

3.3. If you are aware of or believe that any other representative of ours is not complying with Data Protection Laws and/or this Policy you should report it in confidence to the LC for HTC.

4. Other consequences

4.1. There are a number of serious consequences for both yourself and us if we do not comply with Data Protection Laws. These include:

4.1.1. For you:

4.1.1.1. **Restriction/Termination of contract:** Where you are a Worker, failure to comply with our policies could lead to termination of your Worker position with the service.

4.1.1.2. **Criminal sanctions:** Serious breaches could potentially result in criminal liability.

4.1.1.3. **Investigations and interviews**: Your actions could be investigated and you could be interviewed in relation to any non-compliance.

4.1.2. For the organisation:

4.1.2.1. **Criminal sanctions:** Non-compliance could involve a criminal offence.

4.1.2.2. **Civil Fines:** These can be up to 20 million Euros or 4% of the annual club turnover whichever is higher.

4.1.2.3. **Assessments, investigations and enforcement action**: We could be assessed or investigated by, and obliged to provide information to, the Information Commissioner ("**ICO**") on its processes and procedures and/or subject to the ICO's powers of entry, inspection and seizure causing disruption and embarrassment.

4.1.2.4. **Court orders:** These may require the service to implement measures or take steps in relation to, or cease or refrain from, processing personal data.

4.1.2.5. **Claims for compensation:** Individuals may make claims for damage they have suffered as a result of the services non-compliance.

4.1.2.6. **Bad publicity:** Assessments, investigations and enforcement action by, and complaints to, the ICO quickly become public knowledge and might damage the service. Court proceedings are public knowledge.

4.1.2.7. **Loss of business:** Prospective clients might not want to deal with the service if we are viewed as careless with personal data and disregarding our legal obligations.

4.1.2.8. **Use of management time and resources:** Dealing with assessments, investigations, enforcement action, complaints, claims, etc takes time and effort and can involve considerable cost.

5. Data protection laws

5.1. The Data Protection Act 1998 ("**DPA**") applies to any personal data that we process, and from 25th May 2018 this will be replaced by the General Data Protection Regulation (**GDPR**) and the Data Protection Act 2018 ("**DPA 2018**") (together "**Data Protection Laws**") and then after Brexit the UK will adopt laws equivalent to these Data Protection Laws.

5.2. This Policy is written as though GDPR and the DPA 2018 are both in force, i.e. it states the position as from 25th May 2018.

5.3. The Data Protection Laws all require that the personal data is processed in accordance with the Data Protection Principles (on which see below) and gives individuals rights to access, correct and control how we use their personal data (on which see below).

6. Personal data

6.1. Data will relate to an individual and therefore be their personal data if it:

6.1.1. identifies the individual. For instance, names, addresses, telephone numbers and email addresses;

6.1.2. its content is about the individual personally. For instance, medical records, a recording of their actions, or contact details;

6.2. Examples of information likely to constitute personal data:

6.2.1. Unique names;

6.2.2. Names together with email addresses or other contact details;

6.2.3. video and/or photographic images;

6.2.4. Information about individuals obtained as a result of Safeguarding checks;

6.2.5. Medical and disability information;

7. Lawful basis for processing

7.1. For personal data to be processed lawfully, we must be processing it on one of the legal grounds set out in the Data Protection Laws.

7.2. For the processing of ordinary personal data in our organisation these may include, among other things:

7.2.1. the data subject has given their consent to the processing (counselling agreements)

7.2.2. the processing is necessary for the performance of a contract with the data subject (payment of fees and letters to external parties);

8. Special category data

8.1. Special category data under the Data Protection Laws is personal data relating to an individual's race, political opinions, health, religious or other beliefs, trade union records, sex life, biometric data and genetic data.

8.2. Under Data Protection Laws this type of information is known as special category data and criminal records history becomes its own special category which is treated for some parts the same as special category data. Previously these types of personal data were referred to as sensitive personal data and some people may continue to use this term.

8.3. To lawfully process special categories of personal data we must also ensure that the individual has given their explicit consent to the processing.

8.4. To lawfully process personal data relating to criminal records and history there are even more limited reasons, and we must either:

8.4.1. ensure that either the individual has given their explicit consent to the processing; or

8.4.2. ensure that our processing of those criminal records history is necessary under a legal requirement imposed upon us.

8.5. We would normally only expect to process special category personal data or criminal records history data in the context of our client work for reasons of health and safety requirements, safeguarding checks, etc.

9. When do we process personal data?

9.1. Virtually anything we do with personal data is processing including collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction. So even just storage of personal data is a form of processing. We might process personal data using computers or manually by keeping paper records.

9.2. Examples of processing personal data might include:

9.2.1. Using personal data to correspond with clients;

9.2.2. Holding personal data in our databases or documents; and

9.2.3. Recording personal data in client or Worker files.

10. Outline

10.1. The main themes of the Data Protection Laws are:

10.1.1. good practices for handling personal data;

10.1.2. rights for individuals in respect of personal data that data controllers hold on them; and

10.1.3. being able to demonstrate compliance with these laws.

10.2. In summary, data protection law requires each data controller to:

10.2.1. only process personal data for certain purposes;

10.2.2. process personal data in accordance with the 6 principles of 'good information handling' (including keeping personal data secure and processing it fairly and in a transparent manner);

10.2.3. provide certain information to those individuals about whom we process personal data which is usually provided in a privacy notice (counselling agreement)

10.2.4. respect the rights of those individuals about whom we process personal data (including providing them with access to the personal data we hold on them); and

10.2.5. keep adequate records of how data is processed and, where necessary, notify the ICO and possibly data subjects where there has been a data breach.

10.3. Every Worker has an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy.

10.4. Data protection law in the UK is enforced by the Information Commissioner's Office ("**ICO**"). The ICO has extensive powers.

11. Data protection principles

11.1. The Data Protection Laws set out 6 principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:

11.1.1. processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;

11.1.2. collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("purpose limitation");

11.1.3. adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation");

11.1.4. accurate and where necessary kept up to date;

11.1.5. kept for no longer than is necessary for the purpose ("storage limitation");

11.1.6. processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and security").

12. Data subject rights

12.1. Under Data Protection Laws individuals have certain rights (**Rights**) in relation to their own personal data. In summary these are:

12.1.1. The rights to access their personal data, usually referred to as a subject access request

12.1.2. The right to have their personal data rectified;

12.1.3. The right to have their personal data erased, usually referred to as the right to be forgotten;

12.1.4. The right to restrict processing of their personal data;

12.1.5. The right to object to receiving direct marketing materials;

12.1.6. The right to portability of their personal data;

12.1.7. The right to object to processing of their personal data; and

12.1.8. The right to not be subject to a decision made solely by automated data processing.

12.2. The exercise of these Rights may be made in writing, including email, and also verbally and should be responded to in writing by LC for HTC without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. We must inform the individual of any such extension within one month of receipt of the request, together with the reasons for the delay.

12.3. Where the data subject makes the request by electronic form means, any information is to be provided by electronic means where possible, unless otherwise requested by the individual.

12.4. If we receive the request from a third party (e.g. a legal advisor), we must take steps to verify that the request was, in fact, instigated by the individual and that the third party is properly authorised to make the request. This will usually mean contacting the relevant individual directly to verify that the third party is properly authorised to make the request.

12.5. There are very specific exemptions or partial exemptions for some of these Rights and not all of them are absolute rights. However, the right to not receive marketing material is an absolute right, so this should be complied with immediately.

12.6. Where an individual considers that we have not complied with their request e.g. exceeded the time period, they can seek a court order and compensation. If the court agrees with the individual, it will issue a Court Order, to make us comply. The Court can also award compensation. They can also complain to the regulator for privacy legislation, which in our case will usually be the ICO.

12.7. In addition to the rights discussed in this document, any person may ask the ICO to assess whether it is likely that any processing of personal data has or is being carried out in compliance with the privacy legislation. The ICO must investigate and may serve an "Information Notice" on HTC (if the service is the relevant data controller). The result of the investigation may lead to an "Enforcement Notice" being issued by the ICO. Any such assessments, information notices or enforcement notices should be sent directly to LC for HTC from the ICO.

12.8. In the event of a Worker receiving such a notice, they must immediately pass the communication to LC for HTC.

13. Notification and response procedure

13.1. If a Worker has a request or believes they have a request for the exercise of a Right, they should:

13.1.1. pass the call to LC for HTC. The LC should take and record all relevant details and explain the procedure. If possible try to get the request confirmed in writing addressed to LC for HTC; and

13.1.2. inform the LC of HTC of the request.

13.2. The LC for HTC will co-ordinate the services response (which may include written material provided by external legal advisors). The action taken will depend upon the nature of the request. The LC for HTC will write to the individual and explain the legal situation and whether the service will comply with the request. A standard letter/email from HTC services should suffice in most cases.

14. Your main obligations

14.1. What this all means for you can be summarised as follows:

14.1.1. Treat all personal data with respect;

14.1.2. Treat all personal data how you would want your own personal data to be treated;

14.1.3. Immediately notify the LC of HTC if any individual says or does anything which gives the appearance of them wanting to invoke any rights in relation to personal data relating to them;

14.1.4. Take care with all personal data and items containing personal data you handle or come across so that it stays secure and is only available to or accessed by authorised individuals; and

14.1.5. Immediately notify the LC of HTC if you become aware of or suspect the loss of any personal data or any item containing personal data.

15. Your activities

15.1. Data protection laws have different implications in different areas of the service and for different types of activity, and sometimes these effects can be unexpected.

15.2. Areas and activities particularly affected by data protection law include human resources, payroll, security (e.g. CCTV), customer care, sales, marketing and promotions, health and safety and finance.

15.3. You must consider what personal data you might handle, consider carefully what data protection law might mean for you and your activities, and ensure that you comply at all times with this policy.

16. Practical matters

16.1. Whilst you should always apply a common-sense approach to how you use and safeguard personal data, and treat personal data with care and respect, set out below are some examples of dos and don'ts:

16.1.1. Do not take personal data out of HTC's premises (unless absolutely necessary).

16.1.2. Never leave any items containing personal data unattended in a public place, e.g. on a train, in a café, etc and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.

16.1.3. Never leave any items containing personal data in unsecure locations, e.g. in a car on your driveway overnight and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.

16.1.4. If you are staying at a hotel then utilise the room safe or the hotel staff to store items containing personal data when you do not need to have them with you.

16.1.5. Do encrypt/password protect laptops, mobile devices and removable storage devices containing personal data.

16.1.6. Do lock laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use.

16.1.7. Do password protect documents and databases containing personal data.

16.1.8. Never use removable storage media to store personal data unless the personal data on the media is encrypted.

16.1.9. Use confidential waste disposal for any papers containing personal data, do not place these into the ordinary waste, place them in a bin or skip etc, and either use a confidential waste service or have them shredded before placing them in the ordinary waste disposal.

16.1.10. Do dispose of any materials containing personal data securely, whether the materials are paper based or electronic.

16.1.11. When in public place, e.g. a train or café, be careful as to who might be able to see the information on the screen of any device you are using when you have personal information on display. If necessary move location or change to a different task.

16.1.12. Do not leave personal data lying around, store it securely.

16.1.13. When speaking on the phone in a public place, take care not to use the full names of individuals or other identifying information, as you do not know who may overhear the conversation. Instead use initials or just first names to preserve confidentiality.

16.1.14. If taking down details or instructions from a client in a public place when third parties may overhear, try to limit the information which may identify that person to others who may overhear in a similar way to if you were speaking on the telephone.

16.1.15. Never act on instructions from someone unless you are absolutely sure of their identity and if you are unsure then take steps to determine their identity. This is particularly so where the instructions relate to information which may be sensitive or damaging if it got into the hands of a third party or where the instructions involve money, valuable goods or items or cannot easily be reversed.

16.1.16. Do not transfer personal data to any third party.

16.1.17. Do notify the LC for HTC immediately of any suspected security breaches or loss of personal data.

16.1.18. If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to the LC for HTC.

17. Foreign transfers of personal data

17.1. Personal data must not be transferred outside the European Economic Area.

18. Queries

18.1. If you have any queries about this Policy please contact Helen Townsend LC for HTC at www.HTCounselling.co.uk & 07936 714259