

---

## Child in Time Data Protection, Confidentiality and Record Keeping Policies

### Data Protection

We are committed to protecting personal information and being transparent about what we do with it, whether you want to work with us, take up a placement or use our services.

We are committed to using personal information in accordance with our responsibilities. We won't do anything with any service users information you wouldn't reasonably expect. We are required to provide you with the information in this Privacy Notice under applicable law which includes (but is not limited to):

the General Data Protection Regulation (EU) 2016/679 (the "**GDPR**"), and the Data Protection Act 2018 the Privacy and Electronic Communications (EC Directive) Regulations 2003.

Processing of personal information is carried out by Child in Time which is a company incorporated in the United Kingdom with company number 08537835. We are registered with the ICO.

Details requested for running employment checks are stored on a password protected system and can only be accessed by two Child in Time employees involved in managing recruitment and services. When you no longer wish to work for Child in Time your details will be deleted.

If you have any queries about our Privacy Notice, please get in touch with our data protection officer:

Email: [chloe@childintime.co.uk](mailto:chloe@childintime.co.uk)

Phone:07984462415

### Information for Schools re Client (children's) personal data

Child in Time does **not** store personal data from the children who receive counselling in schools. School counsellors are required to collect sensitive personal data in order to carry out their work. This includes information for referral forms, consent letters, counselling reports, client art work, correspondence with other professionals and session notes. This data will be held for a maximum of

---

six years after counselling has ended. We are committed to refreshing and interrogating the rationale for the data we are storing.

### **Consent**

GDPR sets a high standard for consent which is in line with good practice for all therapists. It remains important to obtain explicit consent from the parent/carer of the child receiving counselling. A clear record of consent (signed consent letter) should be stored at school and held by the school link person. Gillick Competency, under which law a young person can receive counselling without parental consent, should be used as an exception rather than a rule and the decision to embark on work using the Gillick Competence framework should never be taken by one individual.

### **Storing data**

Client data will be kept confidential and will be locked either in a physical cabinet at the school or a computer filing system at school. In order to carry out their work and attend supervision for their clients outside school hours, therapists are likely to keep certain files (such as session notes and reports) on their own personal laptop or in a filing cabinet in their home. Laptops will be password protected and home filing cabinets locked. Any personal data held by your therapist will be deleted or shredded (if paper) after a maximum of six years.

### **Session notes**

Session notes that are held by therapists will not include the child's personal data such as name, birth date or address. Instead they will use a code. These will be deleted after a maximum of seven years.

### **Reports**

Reports will include personal data so these should be sent password protected initially after which they can be stored using a code instead of a name. Reports will be held at the school according to their own policy and can be retained (using a code) by the therapist for up to seven years.

### **Emails**

We recommend that therapists are given a school email address (instead of using gmail or other unsecured networks) and that initials rather than names are used when sending emails about a child. Therapists are advised to keep the contents of emails about children to a minimum but cannot

---

be responsible for what incoming information they receive. Any emails received by the therapist will be deleted after the work has concluded.

In the light of changes to GDPR in 2018, we recommend that schools discuss any details of this policy with your counsellor, particularly considering whether current consent letters are compliant and that data storage is discussed when a therapist leaves. We are committed to refreshing the rationale for the data we are storing and for sharing developments with our team.

## DATA PROTECTION

We are all mobile, often working one day here and another there, so it's likely that we're carrying a lot of sensitive, personal data with us. Loss or theft of one of these files would be a serious breach of data protection and we need to do everything possible to guard against this. The first step is to minimise the sensitive data you carry with you. The next step is to use codes, not names for any session notes that you carry (on your laptop for example).

In terms of hard copies, it is essential that your schools give you access to a locked cabinet where referral forms and other personal data is kept. This kind of data, with children's personal details and mental health records on is particularly sensitive and whilst it can be tempting to take hard copies home to reflect on, the risks of these forms being lost or the bag they are in being stolen, makes it essential that they stay in school.

### **Our Policy to protect data:**

Ensure any mobile devices have a lock and password

Use codes instead of client names on session notes

Keep emails to a minimum and don't use names (delete emails sent to you with names)

Password protect any reports being sent by email

Keep all referral forms in school

Check locks before leaving: keep the key in a safe place in school if hard copies

If there is a data security breach please let Chloe know and she will support you the school

*Child in Time is registered with the ICO (information commissioners office) who have further information on data protection.*

## GDPR (Government Data Protection Regulations)

- Ask your school for a school email - they may say you are not an employee so they can't. If this is the case, password protect your emails and send passwords in a separate email.
- Password protect emails if sent from non school emails or use encrypted email accounts such as 'proton-mail'.
- Keep session notes (without names/personal data) for up to 7 years and then delete. NB There is still some discussion about the number of years - UKCP for example do not recommend a specific number of years. But think about why you are keeping old client info. If there is not a valid reason, please delete.
- If you have paper notes, please shred before throwing away.
- Be explicit about confidentiality and data storage with parents/carers at the start.
- Ensure that schools hold the sensitive client referral data which can be accessed by your link person. You only retain session notes without names/addresses etc
- Due to GDPR changes (2018) a client (or the guardian of a client) might make a request to see the information held about them. This is a 'subject access request'. In this instance a therapist will need to weigh up various factors based on advice from the ICO when responding. The school will have a number of days to respond and may have a different view to you re access. Please consider this when writing session notes. Your process notes, with your thoughts and ideas would be better kept separate from the more straightforward 'session themes' which should be clear and limited.