Data Protection and Confidentiality Policy

Document Management

Date Last Updated:	17th October 2022
Version:	1.2
Author:	Zane Wilson
Contact:	zw@cherrycroft.pro

Contents

Document version history				
Document Name:	Data Protection and Confidentiality			
Staff members consulted/part of the review:	Claudia Wilson Zane Wilson			
Author:	Claudia Wilson			
Version	**Date**	**Amendments made**	**By whom (name/job title)**	**Senior approval Claudia Wilson**
1.0	10/10/2018	Initial version	Claudia Wilson	
1.1	10/8/2019	Annual review – formatting added LA Contract section, added key cupboard information, added ICO details, header data	Zane Wilson	
1.2	14/10/2020	Annual review	Melanie Micklewright	
1.3	17/10/2022	Protecting client data GDPR	Melanie Micklewright	

Purpose of Policy

As a therapeutic provider we often deal with sensitive and confidential information that must be handled with great care. We are all responsible for keeping information safe.

Responsible Roles

The Director **Claudia Wilson** is overall accountable for data protection and is the nominated data protection officer registered with the ICO. The operations manager **Zane Wilson** is responsible for ensuring day-to-day implementation and compliance with the policy.

Protecting Client data

1. All workers should ensure they have competed appropriate data security training (GDPR training).
2. All clients must have a paper file and an electronic file which is currently in the form of OneNote.
3. Paper files contain (all must be kept up to date): a front sheet, consent forms, any reports received as paper copies and paper questionnaires. Clients work or drawings completed during the session may also be kept in the paper file.
4. Paper files are to be kept in locked filing cabinet and whoever is the last to leave the office has a duty to ensure that the filing cabinets are locked, and the keys stored in the key cupboard and the key cupboard locked. Paper client records are not to be removed from the premises. No confidential information is to be left out on desks. Any notes taken in note books should be anonymised.
5. The admin office door is to be kept shut and locked during the day when the admin office is unattended.
6. Electronic devices and storage – any device that holds client data like laptops, mobile phones, iPads and tablets, data storage devices, USB's, etc. must be encrypted.
7. As part of our work, we often video record sessions – a copy must be stored on the One Note client record. Video recordings of sessions must be stored on an encrypted device if they are to be viewed at home.
8. All video recorded sessions must have a signed consent form and these must be uploaded to the client record and a paper copy in the client's paper file.
9. Transfer of data – must be done in a secure way that complies with EU/UK legislation.
10. The Cherrycroft email address must be used for Cherrycroft work. Where possible and especially for the transmission of confidential reports or other sensitive email a secure email server e.g., Egress must be used.
11. All e-mails are required to have the usual disclaimer on the footer of the email.
12. Staff are asked to please put an out of office message if they are away.
13. All passwords are to be kept in a secure manner.
14. Important to ensure a careful reading of reports to ensure that the correct names are in the reports and other correspondence.
15. Breaches or possible breaches in protecting confidential information must immediately be reported to Claudia Wilson.
16. Client related information must not be discussed with anyone outside of the Practice unless there are safeguarding concerns then the safeguarding procedure is to be followed.
17. All staff are to be aware that we are obliged to keep information for a prolonged period especially in the case of adopted families.
18. If a member of staff recognises a personal connection to a client, then they will immediately stop looking at the client file and let Claudia Wilson know immediately.
19. The last person to leave the premises is responsible for ensuring that the admin door is closed/locked and that the building is secured and locked.

Bounds of confidentiality

All staff must acquaint themselves with the safeguarding policy and also make the boundaries of confidentiality clear to clients at the start of the intervention – information is held in the strictest of confidence, but we may be obliged to break confidentiality if there are any safeguarding concerns. We will try to include families in our plan to break confidentiality if this does increase any risks.

Contracts with local authorities must be checked carefully for data protection issues. The standard local authority (LA) terms & conditions tend to require data treatment, which is contrary to good practice for therapeutic services, for example:

- Requirement for Cherrycroft to obtain data sharing consent from the LA's clients on their behalf (this is the LA's responsibility)
- Claims of IP ownership over therapy notes and other materials (we keep these confidential except where required for safeguarding concerns, and summarised information that is included in reports)
- Requirements for Cherrycroft to destroy data held about clients at the end of the contract.

These need to be challenged and the LA contract managers referred to the relevant legislation e.g., section 14 of the Children and Young Persons Act 2005.

Notwithstanding the LA T&Cs, for work that is commissioned by social services we need to make it clear that we are required under the terms of our agreements with local authorities and of the ASF that they will receive copies of reports, even though it is the responsibility of the local authorities to make this clear to clients and obtain their consent for their data to be shared.

Protecting Staff Information

Staff contact details must not be shared with clients nor personal details e.g., mobile phone numbers without the express permission of that member of staff.

As a condition of our work, local authorities often ask for therapists/ staff members CVs, copies of degree/relevant courses certificates, professional liability insurance, copies of enhanced DBS certificates, proof of professional registrations (e.g., HCPC) and copy of professional liability insurance documents. Please be aware that we will be obliged to share this documentation with local authorities.

Staff are required to hold an up-to-date enhanced DBS certificate and we suggest that the update service is a convenient way to keep the checks up to date.

We are required to adhere to the safer recruitment policy which is informed by government legislation. Staff are obliged to disclose any changes to professional registrations, or any convictions or cautions received.

Please also keep us updated of any changes to your contact details.

Registration with the Information Commissioner's Office

Cherrycroft is registered with the ICO as a Data Controller as follows:

> Organisation name: THE CHERRYCROFT PRACTICE LIMITED
> Reference: ZA020655

This registration must be kept current. Annually, or when a change to how data is handled is made, compliance with the declaration made to the ICO must be checked.

The General Data Protection Regulation (GDPR) and Data Protection Act 2018

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 introduce new elements to the data protection regime, superseding the Data Protection Act 1998. Practitioners must have due regard to the relevant data protection principles which allow them to share personal information,

The GDPR and Data Protection Act 2018 place greater significance on organisations being transparent and accountable in relation to their use of data. All organisations handling personal data need to have comprehensive and proportionate arrangements for collecting, storing, and sharing information.

The GDPR and Data Protection Act 2018 do not prevent, or limit, the sharing of information for the purposes of keeping children and young people safe.

To effectively share information:

- All practitioners should be confident of the processing conditions, which allow them to store, and share, the information that they need to carry out their safeguarding role. Information which is relevant to safeguarding will often be data which is considered 'special category personal data' meaning it is sensitive and personal

- Where practitioners need to share special category personal data, they should be aware that the Data Protection Act 2018 includes 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information without consent

- Information can be shared legally without consent, if a practitioner is unable to, cannot be reasonably expected to gain consent from the individual, or if to gain consent could place a child at risk.

- Relevant personal information can be shared lawfully if it is to keep a child or individual at risk safe from neglect or physical, emotional or mental harm, or if it is protecting their physical, mental, or emotional well-being.

Monitoring and Review of the Policy

This Policy will be reviewed on an annual basis in August. However, if there are updates before the review these will be forwarded to all members of the team.