Low Farm Therapy Centre Data Protection and Information Sharing Policy

Written by Ruth Lo October 2015

Reviewed August 2017

To be reviewed September 2018

Low Farm Therapy Centre (hereafter referred to as 'the Centre') collects and uses personal information about staff, children, parents and other individuals who come into contact with the Centre. This information is gathered in order to enable the Centre to provide therapy and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the Centre complies with its statutory obligations. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines. Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. Lo and Lo Education, and the trading name Low Farm Therapy Centre, are registered with the Independent Commissioners Office. Ruth Lo acts as the data controller with ultimate responsibility for the data.

The Centre recognises the importance of information sharing in supporting our work with children. However, we understand that it is important that children and their families can be confident that their personal information is kept safe and secure and that we maintain their privacy whilst sharing information when necessary.

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. This policy also relates to information sharing within the Centre and with outside agencies. Our procedures in relation to sharing information with regard to safeguarding are detailed in our Safeguarding and Child Protection Policy.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;

8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Centre is committed to maintaining the above principles at all times. Therefore it will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure staff are aware of and understand policies and procedures

Client documentation storage and sharing within the Centre

- All confidential documentation will be kept in a locked, secure storage facility in the office and/or stored in password protected computer files.
- All members of staff are required to sign a confidentiality agreement when they join the Centre.
- Documentation that is to be discarded should be shredded.

Sharing information with outside agencies

From time to time, the Centre may be required to share information about children with outside agencies. This may be, for example, in connection to their transition to an educational establishment or to access support from other services, such as Child and Adolescent Mental Health Services. Procedures for sharing information with the Social Care Team are outlined in our Safeguarding and Child Protection Policy.

In such cases, the Centre follows the guidance provided in:

'Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers' (HMG March 2015).

We decide whether to share personal information on a case-by-case basis, applying the seven 'Golden Rules' in the guidance:

1. Remember that the Data Protection Act 1998 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.

2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice from other practitioners if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4. Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, there is good reason to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared.
5. Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Decision making follows the procedure outlined in the flowchart in Appendix A.

Information sharing procedure:

When the Centre has decided to share information, and has had the necessary consent, the following procedure is followed to ensure that it is only received and read by the intended recipient(s):

- Check with the agency to establish which named person will receive the information. Alert the recipient to the proposed method of communication and the expected timing.
- Information may be shared directly with the named recipient over the telephone.
- Material travelling by post should be securely packed and marked “Confidential” and sent by Recorded Delivery. A receipt of postage should be retained.
- E-mails should include a rider requesting contact should the email be misdirected and marked “Confidential - For Addressee Only”. “Read receipts” should be kept as evidence as these are acceptable evidence that an e mail has been received and read by the intended recipient. When emailed, documents should be attached as PDF files to prevent alterations being made.
- Where the transport of confidential documentation is required, such material should not leave the therapist’s person.

Retention of Client Records after Discharge.

The Limitation Act 1980 gives the limitation period in which claims must be made. As a general rule a claim cannot be made more than 6 years from the date on which the claimant’s cause of action

accrued. The time will run either from when it happened, or from the date of knowledge. The Department of Health recommends that health records should be kept for a minimum of eight years, and Low Farm Therapy Centre follows this guidance, with exemptions as detailed below:

- **Children:** Based on the fact that a child gains legal capacity from the age of 18, children's records should be kept until the child's 26th birthday.

- **People under a disability:** Whether children or adults, a person under a disability has no time limit on when they can instigate legal proceedings and so their records must be retained for eight years after the person is no longer under a disability. If the person remains under a disability for life, then all records should be retained for life and then eight years after their death. This is based on capacity, and the fact that a client with a disability may not have the capacity to understand that they could instigate legal proceedings, but at any time an advocate could identify a past issue and support them to instigate legal proceedings.

Archived case notes in both paper or electronic form will still be kept in a safe and secure space. In the event of the therapist's mental incapacity, notes on active cases will be handed on to a colleague. As no action can be taken against a deceased person, records can be disposed of in the case of a therapist's death.

Subject Access Requests

Low Farm Nursery and Therapy Centre's procedures for responding to subject access requests made under the Data Protection Act 1998:

Rights of access to information

Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

These procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to the Head of Centre. If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- Passport
- Driving license
- Utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However, with children this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Head of Centre should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The response time for subject access requests, once officially received, is 40 days (not working or school days but calendar days, irrespective of school holiday periods). However the 40 days will not commence until after clarification of information sought.

5. The Data Protection Act 1998 allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

6. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care Professional or school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale.

7. Any information which may cause serious harm to the physical or mental health or emotional condition of the child or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

8. If there are concerns over the disclosure of information then additional advice should be sought.

9. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

10. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

11. Information can be provided on the premises with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints

Complaints about the above procedures should be made to the Head of Centre who will decide whether it is appropriate for the complaint to be dealt with in accordance with the Centre's Complaint Procedure.

Complaints which are not appropriate to be dealt with through the Complaints Procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information. Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk

Appendix A: Flowchart for decisions regarding Information Sharing with Outside Agencies.