ANDERIDA ADOLESCENT CARE

DATA PROTECTION PROCEDURE

As a result of examination of the basic principles of the data protection policy, the following guidance has been formulated.

Recordings

Some information added to the young person's file whilst placed at Anderida is too sensitive to be disclosed, and therefore will be clearly identified and placed in the closed section of the young person's main file.

Anderida staff are required to produce reports which reflect the best possible practice. Reports must be clear, precise, non-judgmental, child friendly and jargon free. You should clearly record the date, time and the name of the author making the entry. If more than one person completed the report all authors names should be clearly signed. The report should include the situation, the intervention; what you decided, said or did, what you advised, whom you informed, what you considered appropriate action to follow etc.

It is necessary to separate the contents of your report so that the recorded facts are clearly distinguishable from your assessment and opinion. If necessary, get into the habit of declaring your judgement by an appropriate opening phrase, "It is my view that", "Carers believe that", "In my opinion" etc.

Clients Access to Records

Clients are able to view all records kept in the daily file, care plan and most documents in the main file (with the exception of those in the closed section) and in general should be encouraged to understand the nature of the recordings the care team do, how these will form part of their history and their right to view and read all documents.

How young people want to receive their documents should be agreed as part of the Conditions of Residency when a young person moves to the home. It is important to be open and transparent but also to recognize the young people's right to live in a house that feels homely, rather than ongoing assessment of their progress. Those in the care plan are particularly child centered and should be shared regularly in the manner in which the young person chooses. Should a young person wish to access a particular document written by Anderida care staff that has not been shared but is within the above remit it should be printed and given to the young person. It is better if a young person is supported to read any recordings, we have written but this is the young person's choice. If a young person is asking to see a file or document from another professional, we would ask that they complete the access to records form in order to give us time to prepare the documents.

Information that cannot be disclosed to the client must be clearly identified by the referring agency or the authors of such documents in any pre-admission and post admission information. It will be assumed that all information not identified thus is accessible to the client. If a client requests access to any closed information the request will be directed to the referring agency. Mentors should also ensure that all documents they deem as particularly sensitive to the clients are also saved in the closed section of the main file and stored securely at all times.

It is part of your duty as a care worker to ensure that each client is aware of their rights to access and to arrange for them to see their file if they so wish. In these circumstances the request must be put in writing by the young person 24 hours prior to obtaining their file. Anderida provides a brief form on which a client may apply to see their file. Managers/senior staff will remove the contents of the closed file in these situations.

Should a significant other/professional who is not part of the Local Authority referring team request written documents they must do so in writing. In order for the document to be shared Anderida would assess 'the need to know' and give their permission based on this assessment. Permission would be given by Managers only and done so where required in consultation with the Local Authority and where appropriate the client. The clients have a right to share documents they have requested with significant others/professionals however they should be encouraged to think seriously about sharing any information and supported to make a good decision in advance of passing on their personal reports.

Where staff are concerned that the young person will cause damage to their file, staff may give recordings in ten sheet sections rather than whole files. Damage to recordings is considered criminal damage, however most recordings will also be held electronically to minimise the loss of data.

Those who may be shown contentious or upsetting material should be offered formal counselling and support after access has been granted.

Data is shared on a need to know basis in line with our safeguarding, disciplinary and whistleblowing procedure. If in doubt about any aspect of data protection it is far safer to ask a senior member of the staff team.

Storage of written records

Confidential files are kept within locked cabinets in the home/head office. Digital recordings are protected by complex passwords held in a locked cabinet at head office. The requirements of the Data Protection Act regarding accurate recording are met in this way.

Storage of DBS

DBS numbers are held in a locked file for all employees.

Length of keeping staff records/disciplinary records

To be held on file for a maximum of six years once a member of staff has left employment with Anderida.

Length of keeping young people's records

Seventy-five years from the date of the young person's birth or if a child dies before reaching their 18th birthday for a period of 15 years from the date of death. These are backed up on a hard drive and held on a spate digital key.

Length of Schedule 4 records

Records must be kept for 15 years from the last date of entry

Staff access to their personnel files/records

Any request needs to be put in writing, clearly stating the reasons for wanting to access files / records.

Digital Storage and Protection

Digital files are kept on a small network of password protected PCs. These PCs are protected from viruses and malicious attack with the use of up-to-date antivirus software and backed up online on a secure, password protected cloud storage server. Files are periodically backed up and protection software is continually updated.

The management and care team can access these files subject to strict protocol. This is as follows;

- The employees have express permission and the correct level of access as defined by the Directors
    - Care and education team (to include senior staff) can only access digital documents whilst at work in the homes, school and office and only have access to the files relevant to the resource or child they are caring for.
    - Managers have remote access to the specific home for which they are responsible and access to the public file which holds Statement of Purpose's, Policies and Procedures and blank organisational documents.
    - Managers who do have access to young peoples and the homes digital records, ensure that they only access these documents on work and personnel computers that are protected from viruses and malicious attack with the use of up-to-date antivirus software.
    - Directors and office staff have access to all the homes paperwork and digital storage.
- Staff that are permitted can only access digital storage on password protected devices
- These passwords are only stored at head office and cannot be accessed through any media device
- No documents can be emailed out of the homes or office without agreement from the office manager or directors.
- Anyone who is forwarding, removing or sharing confidential information without the express permission of the office manager or directors could be subject to disciplinary procedures.

Organisational Emails

Organisational emails are only to be sent from organisational accounts. These will always have a prefix of Anderida, with the exception of the two office emails which hold within the title Anderida Care. These accounts are encrypted for safe exchange of information.

Highly sensitive documents must be sent through the office account only – where they can be further protected by sending on the Egress password protected security ID system.

(Also see Data Protection Procedure, Confidentiality Policy & Mobile Phone Policy)