Data Protection Compliance Policy

Going forward there are certain terms to be aware of with regards to the UK-GDPR. Processing means any operation or set of operations which is performed on personal data, this can include collecting, recording, storage and destruction. Data subjects refer to the person the data refers to. Personal data means any information relating to an identified or identifiable data subject, e.g. name, email address, phone number, DOB or address. Certain personal date is known as sensitive data. We are aware that it is essential to take extra care when processing sensitive data as it could carry significant risk to the fundamental rights and freedoms, these include religion, pollical opinion and ethnicity. We would not process this data without explicit consent or we have a legal basis to do so. All data collected and processed will be done lawfully, fairly and in a transparent manner. It will be collected for a specific, legitimate and explicit purposes and it will be relevant and limited to what we need. Jannicke Ive is this agencies Data Protection Officer.

All information essential to the writing and compiling of Care plans and individual Risk Assessments will be gathered by A Family's Best Friend. We will take personal details, medical history, medication use and personal information pertinent to their appropriate personal and behaviour care. If the information is found to be unnecessary then it will be destroyed appropriately. All information will be obtained through talking to parents and carers and the Service User themselves where appropriate. At the outset of these conversations they will be made aware what it is going to be used for and who will have access to it, they will also sign a consent that they agree to these terms. They will also be informed of their rights to access it and how to go about that. This information will be provided in a written format either via email or in a paper format.

The UK-GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

We will have a month to comply with any access requests and we can refuse or charge for requests that are manifestly unfounded or excessive. If we refuse a request, we must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. We must do this without undue delay and at the latest, within one month.

All information will be held on either of the 2 manager's laptops, which are password enabled. All paper files are kept in the manager's office, in a filing cabinet which has a lock on it. If any personal or android work phones are lost or stolen, the appropriate employees pass system account will be suspended and password changed. All staff work phones except the managers (which are all password protected), only have the contact details for the families and service

users they support and so the potential breach in minimal. If there is a loss of data from the office any persons involved will be alerted. All attempts will be made to recover the data and the individuals involved will be informed of what is missing. We only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we will also have to notify those concerned directly in most cases. We must inform the ICO within 72 hours.

Employees will also have access to the information pertaining to the Service User's they work with through an app on their phones that is password protected. This includes a digital MAR sheet that will be updated as soon as changes occur and go live immediately. The company that provides us with our manager application will have an obligation to ensure our data is safe and secure and can only be accessed by those who need to know. It is the employee's responsibility not to share their password or allow other people to access any personal information on it. All staff know not to use public wifi as it is not secure.

No personal information or confidential material will ever be used on the website or social networking site page. Photos and names of Service Users will only ever be used with parents and carers or the Service Users express permission and the signing of a disclaimer stating to the fact. All employees will also be asked for the same permission in the event it is deemed necessary their information should be shared. Consent for care, administering medication and the use of physical interventions and use of photography is taken via a signature on the app at the initial meeting with parents, carers and service users. As time progresses and our Service users become adults' consent will be re-sought from them or we will check that the parents or carers have power of attorney and the ability to give consent.

At employee supervisions and from feedback gathered from twice yearly questionnaires from parents, carers and Service Users all information will be checked to ensure it is up to date and currently valid. If there are any changes then these will be made as soon as is reasonably possible. Once a year we will review all our care plans to ensure the data is current and relevant.

If information needs to be shared either between employees or with outside agencies, then only information that is deemed essential and beneficial to the Service Users will be. All employees will have access to the information they need on a day-to-day level for the safety and quality of provision provided for the Service Users in their care anything extra will never be stored on paper or electronically by them. When group emails are sent out, we will ensure that all personal addresses are hidden from the other recipients.

All information will be destroyed when it is no longer needed if it becomes obsolete and at the end of the storage limit. The documents will be shredded and disposed of in an appropriate manner. Any Service user we no longer support will have their file closed after 3 years from the last date of support. All documents will be archived and held for a further 2 years before physical copies being shredded and electronic copies deleted. Staff details will be held for 25

years after they have left and then these too will be destroyed. Any information kept on our app will be made inactive.

The office computer is backed up via an online cloud system. Any staff with access to the business email account will know to delete any known spam or junk emails, only to open from trusted sources and leave thigs they are unsure of to the manager to deal with. The business email will not be given out unless it is for business purposes.

Jannicke Ive Nov 2021