FuturesinMind bespoke psychological services

Data Protection Policy

Policy information	
Organisation	**Futures in Mind Ltd**
Scope of policy	This policy covers the following: ▪ General Data Protection Policy ▪ Data Subject Access Rights Procedure ▪ Data Retention Policy ▪ Data Breach Procedure ▪ Processing client data policy **Data processor**: google business operations – g suite (click ***here*** for a link to google GDPR guidance and information)
Policy operational date	25/05/2018
Policy prepared by Data Controllers	Russell Postlethwaite: Russell@futuresinmind.org and Emma Clink: Emma@futuresinmind.org
Date approved by Board/ Management Committee	25/05/2018
Policy review date	25/05/2019

Futures in Mind Ltd. Registered in England and Wales. Number 10461056

Introduction	
Purpose of policy	This policy describes the information that Futures in Mind collects when you use our services, how we use it and where we store it. This information includes personal and sensitive information as defined by the General Data Protection Regulation (GDPR) 2018 and the UK Data Protection Bill 2018. Futures in Mind uses the information we collect in accordance with all laws concerning the protection of personal data, including the Data Protection Act 1998 and the GDPR 2018. In terms of collection, use and storage of personal information, Futures in Mind follows good practice principles as outlined in *Article 5* of the GDPR: ▪ Processing lawfully, fairly and in a transparent manner in relation to individuals; ▪ Collected for specified, legitimate, and explicit purposes and not further processed in a manner that is incompatible with those purposes; ▪ Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; ▪ Accurate and, where necessary, kept up to date every reasonable step must be taken to ensure that personal data that are inaccurate having regard to the purpose for which they are processed are erased or rectified without delay; ▪ Kept in a form which permits identification of data for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data maybe processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical or organisational measures required by the GDPR in order to safeguard the rights of the individuals; and ▪ Processed in a manner that ensures the appropriate security of the personal data against accidental loss.
Types of data	Futures in Mind Ltd holds personal information in relation to clients that includes: ▪ dates of birth ▪ home addresses

	▪ phone numbers ▪ any specific 'needs' whether they are medical; psychological; or other. In addition, Futures in Mind Ltd holds personal information in relation to other clients such as: Schools, course delegates etc. In this case the information held includes: • name and address of school • telephone number • email address All data kept is of relevance and limited to the purposes for which it is collected; namely to support Futures in Mind to undertake the activities for which it is commissioned to do.
Policy statement	This policy outlines the commitment of Futures in Mind to: ▪ comply with both the law and good practice ▪ respect individuals' rights ▪ be open and honest with individuals whose data is held ▪ provide training and support for staff who handle personal data, so that they can act confidently and consistently ▪ Notify the Information Commissioner voluntarily, even if this is not required
Key risks	The main risks as regards data within Futures in Mind fall two key areas: ▪ information about data getting into the wrong hands, through poor security or inappropriate disclosure of information ▪ individuals being harmed through data being inaccurate or insufficient Please see sections below about how much risks are managed through data breach and data security.

Responsibilities	
Company Directors	The overall responsibility for ensuring that the organisation complies with its legal obligations lies with company directors, who are also the named data controllers (see above).
Data Protection Officer	Within Futures in Mind, data protection responsibilities lie with the company directors (Russell Postlethwaite and Emma Clink). Their responsibilities include: ▪ Reviewing Data Protection and related policies ▪ Advising other staff on tricky Data Protection issues ▪ Ensuring that Data Protection induction and training takes place ▪ Notification to the ICO ▪ Handling subject access requests ▪ Approving unusual or controversial disclosures of personal data ▪ Approving contracts with Data Processors
'Staff'	All 'staff' working for and on behalf of Futures in Mind are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. This includes those contracted as 'associates' to undertake work on behalf of Futures in Mind.
Support	Training, guidance and support is offered and available for all who work in and on behalf of Futures in Mind in relation to data protection. This is agreed with the company directors, as appropriate.

Security	
Scope	Data security of Futures in Mind is defined below, as part of this Data Protection policy.
Setting security levels	Futures in Mind follows good practice guidance as issued by 'google g-suite' in relation to data security. This ensures an adequate level of protection is afforded to data held, and is within the legal requirements.
Security measures	Futures in Mind operates appropriate security and password protection measures to ensure data security. Futures in Mind operates a password protection procedure for all emailed electronic data and personal information. All personal IT devices, used for 'business' purposes, are required to have further password protection.
Business continuity	All data is held 'virtually' in a secure 'cloud' storage system that is continually 'backed-up.'
Specific risks	As 'staff' work from home, it is imperative all personal data is either: ▪ Shredded once it has been electronically processed; ▪ Filed in secure, lockable cabinets ▪ Where IT devices are used, such devices are password protected (locked) or closed so that data is not accessible. All 'staff' are aware of "vishing" and "phishing" practices and take appropriate measures to prevent data breaches through this method.
Data Breach Procedure	*A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.* • The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (the Information Commissioner's Office, ICO). • When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we will notify the ICO. • Should this situation occur, we will do this within 72

	hours of becoming aware of the breach, where feasible. • If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will inform those individuals without undue delay. • We will also keep a record of any personal data breaches, regardless of whether we are required to notify. Please also see guidance from the ICO on when breaches should be reported as this is one of the main changes from the current Data Protection Act and GDPR (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/)

Data recording and storage	
Accuracy	Futures in Mind ensures data accuracy; personal information gathered via the Futures in Mind consent form is completed by the client directly such that it is assumed to be accurate at the time of completion. If changes are required, e.g. change of contact details, it would be incumbent upon the client to inform Futures in Mind (see 'Consent Form'). In the case of 'other clients' such as schools, course delegates the same principles apply. As a matter of procedure, 'staff' of Futures in Mind will check accuracy of data held, at times of involvement with the client.
Updating	Futures in Mind adopts a policy of both 'on-going' reviews to ensure accuracy of data and 'formal' annual review in accordance with data retention and storage procedures. ▪ *'On-going'*: ensures accuracy of data that is changed according to client details. ▪ *'Formal'*: an annual overall review of all data held by Futures in Mind to ensure that any data is held within accordance to the data protection principles outlined above.
Storage	All records and personal data are stored electronically in secure cloud storage systems (see google GDPR guidance), and only accessible via 2-step verification systems.
Retention periods	All data held by Futures in Mind is subject to a data retention period of 7 years. Where there is a statutory duty to retain data (e.g. for the purposes relating Education, Health and Care Plans), then Futures in Mind complies with the statutory framework guidance indicating that such records should be retained for 31 years.
Archiving	As all data is held electronically: archiving of such data is not relevant and is subject to review procedures as outlined above.

Right of Access	
Responsibility	Right of access requests are responded to within the legal timeframe of one month. The responsibility for the management of such requests is held by the company directors/data controllers, as named above.
Procedure for making request	You can make a Subject Access Request (SAR) by contacting the Data Controllers (Emma Clink Russell Postlethwaite). Right of access requests must be in writing: this could be paper or email, but must make clear the nature of request in order for fair and swift processing. ▪ We may require additional verification that you are who you say you are to process this request. ▪ Personal information may be withheld to the extent permitted by law. In practice, this means that information may not be provided if it is considered that providing the information will violate the child or young person's vital interests. ▪ If you wish to have your information corrected, you must provide us with the correct data. After we have corrected the data we will send you a copy of the updated information. ▪ if you ask to have your data removed, a decision will need to be made as to whether it should be kept. If we decide that the data should be deleted, it will be deleted without undue delay. ▪ If we refuse a request, you have a right to complain to the Information Commissioner's Office. Guidance issued by the ICO in relation to access request, as outlined on the following link, is adhered to by Futures in Mind. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/
Provision for verifying identity	Where the person managing the access procedure does not know the individual personally there is a requirement for this person to confirm the identity of the person making the request (e.g. passport; utility bill; driving license, etc…) before handing over any information.

Charging	In general, access requests are managed and responded to, free of charge. However, Futures in Mind reserves the right to make a 'reasonable' charge, based on time taken to process and respond, to repeated requests for the same or similar information made by the same individual and/or organisation.
Procedure for granting access	If the request is made electronically, Futures in Mind will endeavour to provide the information in a commonly used electronic format, that is accessible.

Transparency	
Commitment	Futures in Mind is committed to ensuring that Data Subjects are aware that their data is being processed and ▪ for what purpose it is being processed ▪ what types of disclosure are likely, and ▪ how to exercise their rights in relation to the data Such transparency is achieved through explicit information given at the time 'consent' is requested and also via access to policy details and related information (e.g. GDPR guidance documents).
Procedure	Please see above
Responsibility	All responsibility remains with the company directors / data controllers, as named above.

Lawful Basis	
Underlying principles	Futures in Mind is aware of the lawful basis for processing data. Data collected by Futures in Mind is done so via '*consent*:' the individual (in the case of children under the age of 16, the person(s) who are legally responsible for the young person) gives clear consent for Futures in Mind to process personal data for a specific purpose; that which relates to the nature of the business of Futures in Mind. There are also two additional lawful bases applied by Futures in Mind which are 'legitimate interests; and 'contract, depending on the context. For further information, please see: (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/)
Opting out	Even though explicit consent is gained by Futures in Mind to process and hold data, it still respects the rights of individuals to withdraw such consent, at any time, without prejudice.
Withdrawing consent	Future's in Mind Ltd acknowledges that, once given, consent can be withdrawn. There may be occasions where Futures in Mind Ltd has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn. Such cases are rare and a clear explanation will be provided if such circumstances arise.

Employee training & Acceptance of responsibilities	
Induction	All staff who have access to any kind of personal data have their responsibilities outlined during induction procedures
Procedure for staff signifying acceptance of policy	Staff are required to indicate that they have read the all relevant policies before undertaking work for and on behalf of Futures in Mind: this is part of either employment or associate contract arrangements.

Policy review	
Responsibility	The Company Directors / Data controllers hold responsibility for review of this policy.
Timing	The policy will be reviewed, in May 2019.

For more information, please visit the ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

When using a third party data processor, please read the guidelines here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/