Summary

The definitions and policies contained in and related to our Information Security Policy (as listed in that policy) apply to this policy too.

This policy applies wherever personal data is handled, and especially sensitive personal data. We need to handle personal data and some sensitive personal data for the purpose of the services we deliver. Personal data includes day-to-day operational information, such as contact information for schools and attendees for our courses, all the way through to confidential notes relating to cases under our therapy service.

This policy describes how this personal data must be collected, handled and stored to meet our data protection standards and to comply with our legal obligations, such as the DPA (Data Protection Act), which includes the GDPR (General Data Protection Regulation).

Personal Data is defined as any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier. This policy applies to all personal data.

This data protection policy ensures that we:

- comply with data protection law and follows good practice;
- protect the rights of people whose personal data we hold (including Team and Clients);
- are open about how it stores and processes each individuals' data;
- have processes in place to handle requests relating to personal data (especially in accordance with the DPA / GDPR);
- minimise the risk of, and pro-actively secures itself against data breaches; and
- have processes in place to handle data breaches when they are discovered.

Data Protection Law

The Data Protection Act 2018 (DPA), which applies the GDPR under UK law, describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or in any other way.

To comply with the law, personal data must be handled only in keeping with the following requirements:

- kept only when there is a fair and lawful basis to do so;
- be obtained only for specific, lawful purposes;
- sensitive personal data must only be handled if it is covered by certain conditions (such as for providing health and social care services);
- be adequate, relevant and not excessive;
- be accurate and be kept up-to-date;
- not be held any longer than necessary;
- be protected and held with appropriate security in place, with Data Protection Impact Assessments (DPIAs) being completed where appropriate to assess risk relating to the handling of personal data;
- be handled by systems that are "secure by design";
- processed in accordance with individuals' rights so that we can (where obligated) fulfil requests to:
    - understand how we handle and use their data;

    - allow to access, update, remove, stop processing;
    - be provided with the data in a typical format; and/or
    - object to it being processed.
- not be disclosed unlawfully;
- transparency regarding who will handle the data, why and for how long;
- any breaches of personal data must be reported to Information Commissioner's Office immediately, and no longer than 72 hours after being discovered. Serious fines may be issued if adequate security was not in place to protect the data; and
- not to be transferred outside the European Economic Area (EEA), unless compliance with the DPA is maintained by all external parties.

Policy Scope

This policy applies to our whole Team. This also includes suppliers, who are required to fulfil their lawful obligations under the DPA (and the GDPR), including suppliers in countries outside of the United Kingdom or European Economic Area (EEA) who are required to comply with the GDPR when working with organisations or customers in the EEA.

Personal data that has been pseudonymised (e.g., where an ID or key is used instead of a direct identifier) will fall within the scope of this policy if there is a reasonable chance of attributing the pseudonym to a particular individual using any of our Information Systems. For example, if you could work out who an individual is by gathering various information held, even if the name is not held with it.

Data Protection Risks

This policy helps to protect us, our Team and Clients from some serious security risks, including:

- **Breaches of confidentiality and trust**. For instance, highly sensitive information being disclosed inappropriately.
- **Failing to provide transparency** to people regarding how we handle their information. For instance, all individuals should be free to choose if and how we handle/use data relating to them in some instances (not all, depending on legal obligations).
- **Reputational damage**. For instance, we could suffer serious reputational damage if we were found to suffer a breach of sensitive personal information, or to have left information unprotected in a public place.
- **Financial risks** due to penalties for lack of compliance with the GDPR (serious fines are issued where negligence has led to a breach).

Responsibilities

Everyone in our Team has some responsibility for ensuring data is handled and used appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy alongside the other Information Security Policies and the data protection principles contained.

However these people have key areas of responsibility:

- Louise Bombér, our Director, is ultimately responsible for ensuring that we meet our legal obligations regarding data protection.
- The Data Protection Officer (DPO) registered with the ICO (Information Commissioner's Office) is Louise Bombér, who is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from the Team and anyone else covered by this policy.
- Dealing with requests from individuals regarding the personal data that we hold about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle personal data or any other sensitive data.

General Guidelines for Team Members

These guidelines apply for our whole Team when handling Information:

- The only people able to access data covered by this policy must be those who need it for their work;
- Data must not be shared informally. When access to confidential information is required, it must be requested from the information owner in control of that information;
- We will provide training to all employees to help them understand their responsibilities when handling data;
- Team should keep all data secure, by taking sensible precautions and adhering to this policy and those related under the Information Security Policy;
- Personal data must not be disclosed to unauthorised people, either within our organisation or externally;
- Data must be regularly reviewed and updated if it is found to be out of date;
- When data is no longer required, it should be securely removed/erased; and
- Team should request help from their manager or Data Protection Officer if they are unsure about any aspect of data protection.

Required Data Protection Practice

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Technical Manager or Data Protection Officer.

When data is stored on paper, data protection law still applies. Follow the practice under the Information Security Policy section "Paper and Non-electronic Mediums".

The following practice must be adhered to when accessing systems or devices that hold or allow access to **Amber** and **Red** classified data (see the Information Classification Policy):

- personal data, or confidential/sensitive information must not be displayed in any way that might disclose it to unauthorised persons, such as in public places where other people might be able to see your screen (e.g., trains and cafés);
- when data is secured electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts;
- data must be protected in accordance with the Password and Authentication Policy;
- if data is stored on removable media (like CD, DVD, portable hard drive or USB stick) these should be locked away when not being used and they must adhere to the "External Storage" policy detailed in the Information Security Policy;
- data should only be stored on authorised systems and/or devices, including drives, servers and approved Cloud/online services;
- servers containing personal data should be maintained in a secure location with appropriate access

control;
- data should be backed up frequently to an appropriately secure device or service;
- all important backups should be tested regularly;
- data should never be saved directly to computers or mobile devices (including smartphones or tablets) unless they are encrypted and secured in accordance with the Information Security Policy and all those related under it;
- where encryption is not possible, appropriate physical security and access controls must be in place; and
- all servers and computers containing data should be protected by approved security software and an appropriate firewall configuration.

Regarding paper and other non-electronic mediums, the corresponding practice detailed under the Information Security Policy must be kept carefully.

Working with Data

Data is most at risk when it is in use, therefore the following practice is required:

- when working with **Amber** and **Red** classified data:
    - you must ensure the screens of their computers are always locked when left unattended;
    - Personal data must not be shared informally;
    - Personal Data must never be transferred outside of the European Economic Area unless it is to an approved party who complies with the GDPR.
    - you must not save copies of personal data to their own devices unless it is in keeping with the Bring Your Own Device (BYOD) Policy; and
    - always make sure that Information updated on personal devices is backed up and saved to the appropriate Systems so as not to be lost.

Data Accuracy

The law requires us to take reasonable steps to ensure data is kept accurate and up to date.
It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible:

- data must be held in as few places as possible and not be unnecessarily copied;
- Team should take every opportunity to ensure data is updated; and
- where data is copied, it should be maintained with reference to the primary source for that information.

Specific Requirements for Therapy Services, Education Services (Seguridad), Consultations, 7-Day Attachment Lead in Schools Course feedback

When documenting therapy service information, education services information (Seguridad), Consultations, 7-Day Attachment Lead in Schools Course feedback, the following practice must be adhered to:

- In order to anonymise personal data, use the ID code for referencing individuals and never their full name;
- ID codes and relevant names or any information that might directly or indirectly identify an individual

must be saved securely on an encrypted system meeting all the requirements of the Information Security Policy for the corresponding class under the Information Classification Policy;
- Only relevant information may be stored in each document;
- Must be saved only on encrypted devices, or if this is not possible, with appropriate physical security, such as in a locked safe;
- Any sensitive data passed on by Social Services (such as chronologies) must either be sent back securely in keeping with our policies, or destroyed securely on-site by a GDPR compliant shredding company (if held on a physical medium, such as paper) after informing the provider;
- Shared only through an authorised secure email service (see the Information Security Policy for our permitted systems);
- For adults (18 years plus) therapy notes must be kept for 7 years.
- For children (5-17 years) therapy notes must be kept until they are 25 years old.
- Seguridad documents will be saved until children are 25 years old.
- After the child/young person is 25 years old, any investigators will be referred to social services who will have reports saved where required.

Subject Access Requests

All individuals who are the subject of personal data that we hold are entitled to some or all of the following depending on the lawful basis for holding the information:

- to see what information we hold about them;
- to be provided with the information;
- to be able to keep the information up-to-date;
- to have the information removed*;
- to restrict processing of the information (request that processing is stopped or limited);
- to request that they be provided with the information in a typical format* (compatible with other systems);
- to object to the information being processed*; or
- to be informed how we are meeting our data protection obligations.

*Some of the above rights may not apply depending on the "lawful basis for processing" the data. For example, where there is a legal obligation to keep personal data, an individual's request to remove personal data relating to them may be illegal.

If an individual contacts us requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email or post, addressed to the Data Protection Officer. If a subject access request is made, it must be actioned within a reasonable period of obtaining the data and no later than one month.

Disclosing Data for Other Reasons

In certain circumstances data protection legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances we will disclose the requested data. However the Data Protection Officer will ensure the request is legitimate, seeking assistance from the board and from legal advisors where necessary, and also from the ICO if appropriate.

Providing Information

The GDPR requires that we ensure individuals are aware of the following, regarding the processing of their

personal data, by use of a Privacy Notice:

- the purpose for which we are processing the data;
- the retention periods for holding the data;
- who the data will be shared with / processed by (including third-parties who will process the data); and
- how to exercise their rights.

This information must be provided in keeping with these requirements:

- provided at the time we collect the data from the individual;
- be concise, transparent, intelligible, easily accessible, using clear and plain English;
- regularly be reviewed and updated where necessary; and
- where data is obtained from other sources, individuals must be provided with privacy information within a reasonable period of obtaining the data and no later than one month.

We are required to bring to users' attention any new uses of their personal data before processing is started.

Documentation

We are required to document the following regarding personal data we hold:

- the purpose for processing it;
- the retention period we will keep it for;
- the lawful basis for processing;
- any Privacy Policies;
- where it is obtained, stored and all destinations (for example, data flow diagrams); and
- for any special category data, we document:
    - the condition for processing that we rely on in the GDPR (or the Data Protection Bill);
    - the lawful basis for our processing; and
    - whether we retain and erase the personal data in accordance with our policy document.

We are also required to document our processing activities, in a granular way with meaningful links between the different pieces of information.

We are required to conduct regular reviews of the personal data we process and update our documentation accordingly.

Breaches

A data breach is defined in the GDPR as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*".

A few examples of what breaches are include deliberate or accidental access to an unauthorised system, a mis-sent email, or alteration of personal data without permission.

The GDPR requires the following practice concerning personal data breaches:

- to have robust breach detection, investigation and internal reporting procedures;
- to have a process in place to assess the likely risk to individuals as a result of a breach;
- if a breach is unlikely to result in a risk to peoples' rights and freedoms (i.e., if it is very unlikely to cause any risk to people), then you may not need to report it;

- all breaches should be documented; and
- to notify the ICO of a breach as soon as possible after having become aware of it, and no later than 72 hours after (unless you have a valid reason and plan);

Breaches will be considered in the context of the "appropriate technical protection measures being in place" that might effectively limit the risk of mis-use of the information.

To report a breach, the DPO should report this on the ICO's website at ico.org.uk.

Breach Detection

Breaches will be detected as follows:

- By the cyber-security software monitoring and reporting threats, including potential breaches, to us and/or our IT Service Provider.
- By an individual having become aware of a potential compromise of security, or unauthorised access to personal information.

Breach Risk Assessment

If there is any chance people might be negatively affected by a breach that's been discovered, we will report it immediately to the ICO.

The process is as follows:

1. The person who first finds out about the breach contacts the DPO and (if necessary) our IT Service Provider.
2. They consider the potential risk associated with the breach.
   The following is taken from the ICO's website, which is helpful:
   "*In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:*
   "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.""
   So, if there are likely to be any adverse effects on individuals, such as emotional distress, and physical and material damage, then report it.
   For further guidance on this, please refer to ico.org.uk.
3. If any personal information might be disclosed or if there is a risk to any people, then we prepare to report it to the ICO, including the following:
   - a description of the nature of the personal data breach including, where possible:
     - the categories and approximate number of individuals concerned; and
     - the categories and approximate number of personal data records concerned;
   - the name and contact details of the Data Protection Officer (DPO) or another point of contact where more information can be obtained;
   - a description of the likely consequences of the personal data breach; and
   - a description of the measures taken or proposed to be taken to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.
   - The likelihood and severity of the resulting risk to people.
4. If you don't have all the information yet, still go ahead and start to report the breach as you can report

the breach in stages.
For more information, visit this page: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

5. If you decide not to report it due to very low risk to people, then document your justification for this decision.