**Menu of Service Providers/Applications and Relevant Data Protection Information**

**How I keep your data secure**

I take your data protection very seriously and, in addition to the measures listed in this document under each service provider/application, I do the following to ensure your data is protected:

* Anti-virus/Malware Protection on all devices where I store your sensitive data.
* Virtual Private Network (VPN) used if using these devices outside of my home (this is very rare).
* Patch Management – I regular run updates on my devices and software to ensure they have the latest security updates.
* Encryption – I use RSign to send and receive confidential documents and use RMail to send and receive confidential emails. I encrypt the folders on my devices where your sensitive data is stored.
* Back-ups – I regular back up the data on to an encrypted hard-drive.
* Written notes are kept in a locked cabinet.
* I follow guidance from Privacy4 which is an organisation which supports therapists to follow data protection laws and guidelines.

Please refer to the policies and legal documents on my website for further information: <https://www.elliefinch.co.uk/policies>

Logo, company name

Description automatically generated

**FAQs**

**What is the GDPR (General Data Protection Regulation)?**

The GDPR is a European regulation focused on privacy and data protection of EU Citizens. The aim of the GDPR was to create a uniformed approach to the processing and transfer of data across multiple regions, in much the same way as ‘freedom of movement’ was achieved for people across EU countries.

It doesn’t matter where in the world processing of these citizens takes place. If an organisation exists in the USA or Russia; If they process data of EU citizens, then they are forced to comply with the GDPR.

The overarching principle of the GDPR is one of ‘accountability’ and aims to put the control of personal data back in the hands of EU Citizens, including you, me, and your clients.

Each region within the EU has appointed a ‘Supervisory Authority,’ who oversees the governing and implementation of the GDPR within their region. In the UK, this Supervisory Authority is the Information Commissioners Office (ICO).

*(from The Essential Guide for Therapists to Protection of Data’, Catherine Knibbs & Gary Hibberd, 2020)*

**What is the Data Protection Act 2018 (DPA-2018)?**

In the UK, there have been laws governing data protection since 1995. These were in much need of an update due to the advancement of technology and digitisation, and in 2018 the new DPA was introduced.

The DPA cannot be read in isolation of the GDPR

*(from The Essential Guide for Therapists to Protection of Data’, Catherine Knibbs & Gary Hibberd, 2020)*

**Why is it important to know where my data is stored?**

The country your data is stored is significant in terms of which data protection regulations it comes under. If your data is stored in the UK or EU then your data is protected by the DPA-2018 or GDPR. However, if your data is stored outside of the EU or UK then it will be subject to the data protection laws of that country. For example, if the server is based in the US then the data will be held under the US data protection laws which differ from UK and EU data protection laws and may offer less protection to citizens.

**What is ISO27001?**

Possibly the best known and widely used security standard is ISO27001. It contains over 114 controls which an organisation must assess and apply (where appropriate) to their organisation.

The control areas include not only IT systems, but also assess how an organisation hires staff and what training they receive. It asks questions about the development of systems and how changes are applied (not only IT changes, but organisational changes). It looks for assurances around suppliers and asks questions about service levels and contract agreements.

To achieve ISO27001 certification an organisation is assessed over a period of days by an external auditor, who will physically visit the company, interview people and look for evidence of compliance. These audits take a number of days, ranging from 3 to 10, depending on the size of the company. Each year the company is revisited and has to conduct another, mini audit, usually lasting a couple of days.

*(from The Essential Guide for Therapists to Protection of Data’, Catherine Knibbs & Gary Hibberd, 2020)*

**Disclaimer**

The information provided within this document is, to the best of my knowledge, correct at the time of sharing it with you. This is a live document and may be updated at any time to reflect changes in law or growth of the business, and therefore should be revisited regularly to check for any updates. I therefore recommend you read the policies and legal documents available on my website (<https://www.elliefinch.co.uk/policies>) again from time to time. The service providers listed below may also change their own privacy and data protection policies and so I recommend you check them from time to time too. You can withdraw your permission for these apps to be used at any time.

**Online Apps**

A picture containing sky, outdoor, mountain, nature

Description automatically generated

|  |  |
| --- | --- |
| **Name of Service Provider:** | ProReal |
| **Description of service:** | Built using 3D gaming technology, ProReal’s immersive platform helps users create a visual representation of how they experience a situation, enabling them to explore different perspectives, visualise futures and solve problems. Working with trained professionals online or face-to-face, clients use a PC, laptop or tablet to enter a secure, virtual landscape. There, they manipulate avatars and props to create visual representations of real-world scenarios.  Features and Benefits  Clients experience increased self-awareness and rapid empathy-building, leading to improved relationships. The use of ProReal is associated with significant reductions in stress when used in school counselling settings. |
| **Link to data protection info:** | <https://www.proreal.world/privacy/> |
| **Location data is processed (i.e. location of servers):** | UK |
| **Security Standards in place:** | All network traffic is encrypted (TLS)  Proreal has contracts with NHS trusts and had to comply with strict data security checks. However, they have not yet applied for a security standard such as Cyber Essentials (CE) , Cyber Essentials plus (CE+) or ISO27001:2013/17  Data can also be stored locally on the client’s device and shared with the counsellor via a video platform.  ProReal have stated via email to me that “ProReal does not own/have access to user world data… all data belongs to [the] client. We need to store data on the server so online work can be done, but it cannot be accessed beyond the client and facilitator attached to this world.” |
| **Limitations:** | ProReal is not yet ISO27001 certified |
| **How Ellie Finch will protect your data if you use this service provider/app:** | I can disable a client’s worlds outside of their sessions so that the worlds cannot be accessed outside of their session time. |
| **What you need in order to access the app:** | ProReal can be accessed using a web browser or can be downloaded on to your device. |
| **Having read the above information, please indicate if you are happy to use this app/service provider:** |  |



|  |  |
| --- | --- |
| **Name of Service Provider:** | Virtual Sandtray App |
| **Description of service:** | Virtual Sandtray is a new media interpretation of a physical sandtray. Just a few of the capabilities offered beyond a physical tray are a multitude of models (over 5000), ability to save and send trays, record videos and take screenshots and special effects, such as fire, weather and animation. |
| **Link to data protection info:** | <https://sandtrayplay.com/newsite/privacy-policy/> |
| **Location data is processed (i.e. location of servers):** | US based app. Uses Apple’s Cloud. But I chose to save your date locally on my device therefore it is not in the Cloud. |
| **Security Standards in place:** | When you download the client app via the Apple store, Apple will have data that you have downloaded the App. See Apple’s privacy policy here for more information: <https://www.apple.com/legal/privacy/> |
| **Limitations:** | Choosing not to save on cloud means that if I lost my iPad, for example, the data would be lost. |
| **How Ellie Finch will protect your data if you use this service provider/app:** | Saving sand trays locally on my iPad. Not using client’s real name in the app. |
| **What you need in order to access the app:** | Virtual Sandtray is designed to run on recent versions of Apple's iPad platform with the minimum hardware version being the Air.  We have various test devices, which includes iPad Air, Air2, all iPad Pros and iPad 2018.  You can download the client app for free here: <https://apps.apple.com/us/app/virtual-sandtray-client/id1519269015> (please note you will only be able to access the sandtray app during your session)  If you do not have an iPad you can use this app in sessions via me screen sharing and you directing me what to do. Another alternative is to use the Simply Sand Play app (see below) which works on most devices. |
| **Having read the above information, please indicate if you are happy to use this app/service provider:** |  |

A screenshot of a video game

Description automatically generated

|  |  |
| --- | --- |
| **Name of Service Provider:** | Simply Sand Play |
| **Description of service:** | Simply Sand Play is a secure and effective telehealth tool that allows counsellors to practice sandtray therapy with clients — virtually. |
| **Link to data protection info:** | <https://simplysandplay.com/privacy-policy>  <https://www.sentrylogin.com/sentry/site_tou.asp> |
| **Location data is processed (i.e. location of servers):** | Simply Sand Play state that no data is held by them. When a client accesses the application they do so using a password I provide them and then any creative activity produced by the client is saved locally on their device and not in a Cloud anywhere.  Only the clients IP address will be logged by Simply Sand Tray when the client accesses the browser or downloads the app. |
| **Security Standards in place:** | Sentry Login run the member system for Simply Sand Tray.  Sentry Login stated in an email to me that, “While [the ISO27001] certification is not in place, the essence of its requirements are nonetheless all met by Sentry”  <https://www.sentrylogin.com/sentry/site_tou.asp> |
| **Limitations:** | Simply Sand Play currently only allows the previous sandtray made by a client to be saved on their device. This means that the best way to ‘save’ sandtray creations is to take a screenshot and save that image locally. |
| **How Ellie Finch will protect your data if you use this service provider/app:** | Simply Sand Tray can be shared with clients by screen sharing or by giving them access to the Simply Sand Tray account with a password. Once the Sandtray has been accessed it is based locally on your device and is not in the Cloud online anywhere. |
| **What you need in order to access the app:** | There are multiple ways in which Simply Sand Play can be accessed. (using Chrome, Microsoft Edge or Firefox browsers; installable version for Windows PCs or Macs; iOS app for iPads/iPhones) so the chances are very good that it will work on most devices. We cannot guarantee that every device will run Simply Sand Play because some devices may simply be too old. |
| **Having read the above information, please indicate if you are happy to use this app/service provider:** |  |

**Communication methods**

Text, logo

Description automatically generated

|  |  |
| --- | --- |
| **Name of Service Provider:** | Frama (RSign) |
| **Description of service:** | Secure document signing service |
| **Link to data protection info:** | <https://www.frama.co.uk/news/single/who-is-frama/> |
| **Location data is processed (i.e. location of servers):** | EU (Switzerland) |
| **Security Standards in place:** | Frama is certified for IT security as per ISO 27001 and FIPS 140-2 Level 3, the highest security requirement for Cryptographic Modules. |
| **Limitations:** | Do not reply directly to any RSign emails you receive – those emails do not go to me |
| **How Ellie Finch will protect your data if you use this service provider/app:** | I shall store documents I receive from you via RSign in accordance with my data protection policy. |
| **What you need in order to access the app:** | Nothing – simply follow the instructions in the RSign emails. |
| **Having read the above information, please indicate if you are happy to use this app/service provider:** |  |



|  |  |
| --- | --- |
| **Name of Service Provider:** | Protonmail |
| **Description of service:** | Secure email service |
| **Link to data protection info:** | <https://protonmail.com/security-details> |
| **Location data is processed (i.e. location of servers):** | EU (Switzerland) |
| **Security Standards in place:** | Protonmail’s data centers are ISO27001 certified.  The company it not currently ISO27001 certified.  <https://protonmail.com/support/knowledge-base/is-protonmail-gdpr-compliant/> |
| **Limitations:** | You need to also have a Protonmail account (which is free to create) in order to send an encrypted email to my protonmail account: [ellie.finch.secure.email@protonmail.com](mailto:ellie.finch.secure.email@protonmail.com). |
| **How Ellie Finch will protect your data if you use this service provider/app:** | Using Protonmail accounts to communicate with each other will ensure that our communication is end-to-end encrypted. If you email me using a Protonmail account I shall reply using my Protonmail account. |
| **What you need in order to access the app:** | Protonmail account (sign up for free here: <https://protonmail.com/> ) |

|  |  |
| --- | --- |
| **Name of Service Provider:** | Outlook ([ellie.finch.therapy@outlook.com](mailto:ellie.finch.therapy@outlook.com)) |
| **Description of service:** | Email Service |
| **Limitations:** | This email address is not end-to-end encrypted so please do not send personal/confidential information to me via this email address. |
| **Having read the above information, please indicate if you understand that sending emails to Ellie Finch’s outlook.com email address will not be as secure as sending them via a Protonmail account to Ellie’s Protonmail account:** |  |



|  |  |
| --- | --- |
| **Name of Service Provider:** | Zoom |
| **Description of service:** | Video Conferencing Platform which provides whiteboard and screen sharing facilities |
| **Link to data protection info:** | <https://explore.zoom.us/privacy-and-security> |
| **Location data is processed (i.e. location of servers):** | I have Customised the data centre regions for meeting/webinar data in transit on my account to Europe (Germany, Ireland, Netherlands) and US (it is not possible to opt out of the US) |
| **Security Standards in place:** | Zoom state that they are GDPR compliant: <https://explore.zoom.us/privacy-and-security> |
| **Limitations:** | Under events out of our control servers may be used outside of the EU and be subject to the data protection laws of that country. For example, if the server is based in the US then the data will be held under the US data protection laws which differ from UK and EU data protection laws and may offer less protection to citizens.  Zoom does not have an ISO27001 certificate, although they state that they are GDPR compliant. |
| **How Ellie Finch will protect your data if you use this service provider/app:** | I optimise Zoom’s security settings by enabling the passcode and waiting room options. I have also enabled the new end-to-end encryption feature.  I shall save any whiteboard/screenshots from Zoom locally and ensure no identifying information is present. |
| **What you need in order to access the app:** | I’ve enabled Zoom’s new end-to-end encryption service so, if you haven’t already, you will need to download the zoom application to join the call (should only take a few minutes). It should be the first one on the list here ‘Zoom Client for Meetings’: <https://zoom.us/download> |
| **Having read the above information, please indicate if you are happy to use this app/service provider:** |  |
| **Please indicate if you are happy for whiteboard and screenshots of work done in Zoom to be anonymised and saved locally by Ellie** |  |
| **Please indicate if you would like the sessions to be via an alternative platform (if you select this option, I shall discuss possible options with you):** |  |
| **Please indicate if you do not want to use an online platform and would prefer the sessions to be via phone:** |  |

|  |  |
| --- | --- |
| Name: |  |
| Signature: |  |
| Date: |  |
|  |  |
| Name: |  |
| Signature: |  |
| Date: |  |