Issues to consider for storing, transferring and deleting Theraplay® videos and written data - UK 2018

All Theraplay® students and practitioners must adhere to the EU General Data Protection Regulation (GDPR) and provide clients with a privacy notice which details what data you are collecting and why, how it will be stored and transferred, and how and when it will deleted.

The Theraplay® Institute and the UK Theraplay® leadership group are not responsible for your data protection practices or any breaches. The following information is given as prompts for your own investigations and decision making.*

There is a lack of clarity around issues of data protection and confidentiality within the therapeutic professions in the UK. Your professional body may issue guidance on subjects such as registering with the Information Commissioner's Office (ICO), how to store written records, how long to keep records, who can request your written or video data, using a secure email platform, setting up a professional executor (person who is responsible for your notes if you are ill or unable to return to work). You will need to consider these and other issues and have clear procedures in line with your professional body's guidance, workplace requirements and/or personal practice policies.

If working for an organisation, you could refer to your organisation's policies on data protection and online security and consult with your manager and IT department to agree the best practice in your setting. Different local authorities and agencies have different acceptable practices for sharing data and many do not permit an internet-based system. You will need to find out your local supported method(s) and consult your organisation's manager and IT advisor to devise a system if one does not already exist. This can take time to establish but, as you will be dealing with very sensitive data, it is vital that you have an agreed and documented data procedure.

There will always be a way. Whatever you decide, your procedures must be communicated clearly to those giving consent.

Written consent for filming, video sharing, and note taking must be obtained from your clients and work organisations (as well as the local authority, if applicable). See document *3b Consent and Contact Form sample* and document *3c Privacy Statement sample* for suggestions.

Storing and carrying data

As a practicum student or Theraplay® practitioner, you will devise your own way of capturing video footage of your sessions and MIMs. This might be on a camera or a portable device (but should not be a mobile phone). You will also devise your own practices for producing and storing written materials whether these are handwritten or electronic notes. At times, you may need to carry written and/or video data from your home or office to a family home or other setting, and it is important that these are stored and transported in a secure way which maintains confidentiality for the family and ensures that access is restricted.

You should consider keeping video files on an encrypted SD card and/or transferring them to a password protected hard drive or flash drive which is then stored in a locked, unmarked cashbox (putting a 'confidential' sticker on the box will only attract attention). Written documents could also be transferred to a hard drive in the same way.

Passwords should be long and complex so that it is highly unlikely that anyone else could work them out. You might consider using a password manager app for storing multiple passwords. You are likely to store printed papers in a locked filing cabinet, ideally in a locked office and should consider storing video files separately from family files so that the two cannot be matched. You should ensure video files are named by an identifier that only you will recognise.

Transferring data

Many practicum students and Theraplay® practitioners receive supervision remotely using live video interactions such as Skype or Zoom. You will need to agree a secure way of transferring videos to your supervisor.

Videos of MIMs and family sessions are much too large to be sent by email. Transferring videos electronically through a secure transfer system such as WeTransfer, posting encrypted USB sticks or using Dropbox or other Cloud system (with storage located in the EU) are among the more secure methods to consider. See document *5 How to reduce video size before sending* for instructions on how to do this.

You could investigate a secure email platform, eg. Hushmail or Egress, for sending smaller files such as session supervision forms and consent forms.

Deleting data

In the UK, it is currently usual practice for Theraplay® students and practitioners to keep video data for the duration of a Theraplay® case and then to delete files within 3 months of the case being closed, although your organisation may have a longer or shorter time limit. An exception to this deletion schedule would be where the family (and local authority, if applicable) has agreed for a Theraplay® trainer to use the videos for training purposes. Your supervisor should have agreed with you how and when he/she will delete the videos used in supervision sessions (usually directly after the supervision). See document 3a *Supervision Agreement sample* for a suggested contract with your supervisor.

You will also need to agree with all parties when any written notes and session supervision forms are deleted. A number of therapy and counselling organisations suggest six years beyond the child's 18th birthday but this is not for all cases. Children who have been in care or are adopted have special laws applicable to their records (see The Children and Families Act 2014). Again, you need to agree your procedures with your organisation, local authority or commissioning agency.

Deleting a file and emptying the recycle bin on your computer does not mean that the file is no longer retrievable unless you are using an Apple system. It simply means that the operating system has removed it from your view, (imagine your computer data is a chapter book and deleting a file is like ripping out the contents page - the chapters still exist in the same places.) For someone who knows how, retrieving files deleted by the operating system is a fairly simple task. You will need to find a more permanent method of erasing data. The most secure way is to physically destroy the hard drive but of course this isn't a route you can follow while still seeing a family. A digital shredding option will provide sufficient security. This process involves overwriting each file or folder multiple times with random information, rendering it extremely difficult to recover. There are several such tools available, including Eraser which is a freeware file shredder. Given enough resources and time it may still be possible to retrieve the original data, but it will be hidden among enough 'noise' for it to be a very expensive process.

It is also your responsibility, and in line with your organisation's policies, to ensure all data is non-recoverable from your media equipment (including laptop, phone, camera) which has been discarded, passed on, or sold to a third party.