Video Interaction Guidance
Data Collection System (DCS)
Data Policy & Privacy Notice

June 2025

Introduction

The Data Collection System (DCS) was created, and is managed, by the Association of Video Interaction Guidance UK (AVIGuk). The DCS allows Video Interaction Guidance (VIG) practitioners to collate standardised data on the delivery of VIG with their clients. At an individual level it helps practitioners, and their clients, assess client progress. At a service level it helps the evaluation of VIG and provides evidence for funding VIG expertise. At an AVIGuk level it helps promote VIG and demonstrate its efficacy.

The DCS is based on a data collection tool called KoboToolbox developed by Kobo, a non-profit technology company. Kobotoolbox is used all over the world by organisations like the UN, the World Bank and the International Committee of the Red Cross.

The DCS holds various data on Practitioners and their Clients. This document sets out how that data is stored, managed and used. For the purposes of the European Union General Data Protection Regulations (**GDPR**) and/or United Kingdom's Data Protection Act 2018 (**DPA**), AVIGuk is a **controller** in relation to the Personal Information it collects on practitioners and that practitioners collect from clients. Practitioners and their services are considered **data processors**. When copies of data are made by a practitioner's service, for use by a practitioner's service, that data becomes the responsibility of the service to which the practitioner belongs, to be managed in accordance with their data policies, and to which it is expected their clients will have consented. AVIGuk does not process practitioner or client Personal Information for any purpose other than stated in this document

Please read this document carefully to understand our policies and practices regarding your information and how we will treat it. practitioner and client data should only be collected and used when they have expressly agreed by signing a consent form.

If you are a client or practitioner and have questions about this document or if you wish to exercise your rights, contact Charles Baillie at dcs@videointeractionguidance.net

1. Data Privacy

This section details what personal information we collect from practitioners and clients, and how we collect, store and us it. Practitioner and client data are collected and managed differently.

1.1 Client Data

How
Client data are collected by practitioners during VIG intervention – at a minimum consisting of two face-to-face sessions. During these sessions data are entered by the practitioner directly into an electronic form, which is accessed through a web browser or Android app, on a laptop, tablet or smartphone. During completion the form can be saved in the browser cache. Once the form is complete, the data are submitted to the database and data are cleared from the cache. All data are encrypted in transit to the server and at rest on the server. Practitioners can also save a PDF copy of the client's responses, which can also be shared with clients. These PDFs should be stored on a service issued device in accordance with that service's policies.

What
Only the minimum data required to assess client progress are collected through the form. The data collected includes information about the client's child's age group (pre-birth, 0-2, 2-4, 5-11, 11-18 years), other support they may be receiving, qualitative data on the client's perspectives of their child and their relationship, and scores from standardised clinical measures. The name of the client's practitioner as the person conducting the sessions is recorded, as is the practitioner's email address and service name. No personally identifiable client information like name, address, date of birth, or special category data like race, religion, sexual orientation is ever requested through the DCS.

Pseudo-anonymisation
All client data in the DCS are **pseudo-anonymised**. This is achieved using Unique Identifiers (UID) that are assigned to each client. Practitioners can enter a UID that they may have generated on their own service's systems, or they can use a UID generated within the form. It is the responsibility of participating organisations/services to maintain records, in compliance with their own policies, to reconcile UIDs entered in the DCS, and client details stored on their own systems.

Free text fields
Free text fields within the form are necessary for therapeutic interpretation. Yet, they present minor risks to pseudo-anonymisation and inadvertent collection of special category data. This risk is mitigated in the following ways:

- Before using the DCS practitioners are provided with training and materials, which includes information on compliance with pseudo-anonymisation and data collection procedures.
- Practitioners must acknowledge their understanding of pseudo-anonymisation and accidental disclosure is at a level that will ensure compliance with pseudo-

anonymisation and data collection procedures as they relate to the DCS by signing the Terms and Conditions of Use of the DCS.

- Once per quarter an audit of the data is conducted to ensure compliance with pseudo-anonymisation and data collection is being achieved. Non-compliant records will be modified, such as by replacing a name with the record UID and reported to the relevant service lead. Corrective measures such as further training will be provided to practitioners by AVIGuk.

Storage

Client data are stored on KoboToolbox servers hosted on Amazon Web Services. The DCS uses KoboToolbox's EU servers located in Ireland. More information about Kobo's robust data security measures can be found here. AVIGuk has a Data Protection Agreement with Kobo.

AVIGuk will never download and write copies of row level data to disk on personal computers - data will be retrieved using the KoboToolbox API, aggregated in memory and then saved. Periodically, a backup of all records will be made and stored in AVIGuk's Google Workspace. A backup will only be used to restore data on KoboToolbox in the unlikely event of data loss (Kobo databases are themselves backed up daily).

Services may download and store their data according to their own policies and procedures.

Access

Authorised personnel at AVIGuk have administrative access to all DCS records. AVIGuk will only access client data to correct records, delete or transfer records in response to a request, conduct audits or undertake analysis. Access to data will be through the KoboToolbox user interface or through Kobo's API.

Practitioners do not have access to the data they submit to KoboToolbox, other than PDFs they can optionally save before submission. Certain practitioners, nominated by their service, have read access only to records submitted by members of the service, i.e. they will act as data support for their service. This will typically be a service lead or data analyst. Through these nominated practitioners, data may be downloaded from Kobo but then must be managed in accordance with their service's data policy.

Anyone, whether from AVIGuk or a participating service, accessing data through their Kobo account should use 2FA enabled access.

Use

Client data are used differently by practitioners, services and AVIGuk.

Practitioners are primarily interested in therapeutic outcomes. That is, to see improvements in parenting attitudes and their client's relationships with their children. Client data is used to measure that progress by assessing qualitative and standardised measure data between two (or more) sessions. Clients will also be interested in seeing and understanding their progress. Practitioners may de-pseudo-anonymise client data on their own service's systems, in accordance with their service's data policy, to be able to assess their clients progress alongside other therapeutic and contextual information stored on those systems.

Services use aggregated data across all their clients to assess the efficacy of VIG, sometimes in combination with other interventions. This supports funding decisions toward training for practitioners on therapeutic interventions that maximise client outcomes. Analyses will be different between different services and may involve qualitative analysis and measuring improvements in goals or measures.

AVIGuk also uses aggregated data but from across all records from all services. Robustly demonstrating the efficacy of VIG as an intervention that helps to promote stronger relationships using large, national samples, helps AVIG attract funding to support research, develop training, and deliver ongoing professional development. Analysis at this level will combine qualitative and quantitative methods. All personal information, such as practitioner name and email address will be removed from client records before being used for analysis.

1.2 Practitioner Data

How
Practitioner data are collected twice: once when they consent to using the DCS (also through a KoboToolbox form) and once within the client form when the practitioner is conducting a VIG session. All data are encrypted in transit to the server and at rest on the server.

What
Only the minimum data required for practitioners to give consent to use the DCS and agree to the terms and conditions of use, and to match practitioners and their service to a pseudo-anonymised client record are collected through the forms. The consent form collects the practitioner's first name and surname, business email address, the name of the practitioner's service and the practitioner's signature. The client form includes the practitioner's name and the name of the practitioner's service.

Storage
As with client data, practitioner data are stored on KoboToolbox servers hosted on Amazon Web Services. The DCS uses KoboToolbox's EU servers located in Ireland. More information about Kobo's robust data security measures can be found here. AVIGuk has a Data Protection Agreement with Kobo.
AVIGuk will never download and write copies of row level data to disk on personal computers - data will be retrieved using the KoboToolbox API, aggregated in memory and practitioner data removed, then saved. Periodically, a backup of all records will be made and stored in AVIGuk's Google Workspace. Backups will only be used to restore data on KoboToolbox in the unlikely event of data loss (Kobo databases are themselves backed up daily).
Services may download and store their data according to their policies and procedures.

Access
Authorised personnel at AVIGuk have administrative access to all DCS records, including practitioner consent forms. AVIGuk will only access practitioner data to correct records, delete or transfer records in response to a request, or conduct audits, i.e. to ensure practitioners submitting data have agreed to the Terms and Conditions of Use and have received appropriate training. Access to data will be through the KoboToolbox user interface or through Kobo's API.

Anyone, whether from AVIGuk or a participating service, accessing data through their Kobo account should use 2FA enabled access.

Use
Practitioner data will not typically be used other than to correct or retrieve submitted records, and for periodic compliance audits. An example of retrieving a record could be that a practitioner submitted data but did not note the client UID. The practitioner would request support from AVIGuk or from the nominated data support officer within their service who has access to their service records, who would then use the practitioner's name to look up submissions on the date in question and retrieve the UID.

1.3 Service Data Processors

Nominated personnel from each service are given read access to all their service records and will act as data processors for their service. These access controls are managed by AVIGuk using the KoboToolbox access management system. This allows services to 'self-serve' common data requests such as data retrieval/download. When data are downloaded by services, data must be managed in accordance with their service's policies.

Nominated persons are required to create a KoboToolbox account. The DCS will not hold any data that relates to KoboToolbox accounts, but service data processors should familiarise themselves with Kobo's privacy notice.

Service data processors accessing data through their Kobo account should use 2FA enabled access.

2. Data Security

Several measures are taken to secure personally identifiable data held on the DCS from unauthorised access, disclosure, modification, or destruction. These are at the level of the system (i.e. KoboToolbox), in the design of the form, and management of the DCS including access controls. In the event of a breach, affected individuals will be notified as required under GDPR Articles 33 and 34.

System
Confidentiality, integrity and availability features used by KoboToolbox are described here. This includes measures like data back-ups and data encryption when the data are submitted or downloaded from KoboToolbox or at rest on the server (disk-level encryption). KoboToolbox has 2FA and all users of the system from AVIGuk or from services, i.e. nominated personnel, should have it enabled.

Form Design
The design of the form maximises security by:

- **Pseudo-anonymisation (see 1.1 above)**
  Use of UIDs means clients cannot be identified directly. UIDs are generated within the form or practitioners can use a UID that they have already generated elsewhere, perhaps on one of their service's systems. Making UIDs easy to use and

providing an inbuilt generation method means UIDs will be used more effectively. Practitioners are provided with guidance on using UIDs and ensuring personal information is not entered into free text fields.

- **Data Minimisation**
  Only data that is required to guide VIG practice and to assess client progress is collected. Together the data collected could not be used to identify and disclose information on individual clients. Practitioners may be identified individually in their professional capacity, but no special category or other personally identifiable information are collected on practitioners.

Access Control
Only one or two people from each service will be able to access their services' data. Access will be read only to ensure data are not mistakenly deleted or modified. The project is shared with nominated personnel using their KoboToolbox username, for which they will need to sign up, and the data that is shared with those persons is restricted using the service name field within the database.

3. Data Retention

Client data will be stored on the DCS for a minimum of 4 years unless data has been aggregated for analysis sooner. This retention period allows for analysis of the data to support service funding cycles, which may be over multiple years. At the AVIGuk level, a sufficient sample needs to be achieved to have confidence in analysis at the national level. It is expected that this will take a minimum of 4 years.

Practitioner consent form data will be retained for as long as practitioners use the DCS. Should a practitioner cease to use the DCS, for example they move to a service that does not use the DCS, then consent form data will be removed. Practitioners should inform AVIGuk Practitioner data that is associated with a client, i.e. practitioner name, email address and service provider, will be retained alongside the respective client data for as long as the client data is retained - up to a period of 4 years.

4. Consent

Our lawful basis for processing client and practitioner data under GDPR Article 6(1)(a) is their explicit consent.

Both clients and practitioners must explicitly consent to their data being managed in the manner and used for the purposes described in this document. Clients are provided with hard copies of this document and a bulleted summary, which they are asked to sign to provide consent. Client consent forms are retained by the client's service, separately to the DCS. Practitioners sign a digital consent form also on KoboToolbox. The consent form includes a summary of this document and a Terms and Conditions of Use.
If a client does not consent for their data to be collected through the DCS, practitioners may use a hard copy of the online form and store it according to their services' policies and procedures.

5. Privacy Rights

Both clients and practitioners that have their data collected through the DCS may exercise several specific rights related to how their data is processed. These may be exercised at any time.

- **Right to restrict processing:** If clients or practitioners believe that their Personal Information is inaccurate, that our processing is unlawful, or that we do not need your Personal Information for a specific purpose, they have the right to request that we restrict the processing of this Personal Information. They also have the option to request that we stop processing their Personal Information while we assess their request. If they object to our processing (per their right to object as described below), they may also request that we restrict processing of Personal Information while we make our assessment.
- **Right to object to processing:** Clients and Practitioners have the right to object to processing of Personal Information which is based on our legitimate interest by referencing their personal circumstances that makes them want to object to the processing on this ground.
- **Right to data portability:** Clients and Practitioners have the right to ask that we transfer their Personal Information to another organisation or that we transfer it to them.
- **Right to deletion:** Clients and Practitioners can request that their data be removed from the DCS at any time. Clients should request through their practitioner and/or service in the first instance. Practitioners should submit a request to AVIGuk. Deletion requests will be processed by AVIGuk within 14 working days. Client data that is deleted from the DCS may still be retained by the client's service on their systems and clients should discuss this with their practitioner. Practitioners that request their data be deleted from the DCS will no longer be able to use the DCS.