Data sharing agreement

Between:

The Royal College of Speech and Language Therapists

and

ORGANISATION NAME

Introduction

A data sharing agreement between the parties sending and receiving data forms part of compliance with the accountability principle, under the GDPR and the Data Protection Act 2018.

A data sharing agreement:

- helps all the parties be clear about their roles;
- sets out the purpose of the data sharing;
- covers what happens to the data at each stage;
- sets standards;
- provides a framework to help all parties meet the requirements of the data protection principles.

What is included in a data sharing agreement:

1. Parties to the agreement
2. Purpose of the data sharing initiative
3. Organisations involved in the data sharing
4. Sharing data with another controller
5. Personal data items being shared
6. Lawful basis for sharing
7. Special category data, sensitive data or criminal offence data
8. Access and individual rights
9. Information governance arrangements
10. Under what circumstances will the data be accessed?
11. How will the data be stored?
12. How will the data be returned / destroyed?
13. Review frequency
14. Further details (Annex)
15. Signatures

Data sharing agreement

1. Parties to the agreement:

Data controller: Royal College of Speech and Language Therapists **Address:** 2 White Hart Yard, London, SE1 1NX **Phone:** 0207 378 3018 **Email:** dpo@rcslt.org	**Data controller:** ORGANISATION NAME **Address:** _____ **Phone:** _____ **Email:** _____

2. Purpose of the data sharing initiative:

Primary aims:

For practising speech and language therapists:

a) increase reflective practice leading to improvements in patient care, professional development and informing clinical decision making

At a service/local level:

b) demonstrate the impact of speech and language therapy
c) inform service change/quality improvement
d) inform resourcing decisions
e) benchmark the effectiveness of speech and language therapy services
f) inform commissioning
g) ensure services are of good quality for service users and sustainable for the future

Secondary aims:

At a national level:

h) provide evidence to present to commissioning and funding bodies about the value of speech and language therapy
i) demonstrate how the speech and language therapy profession contributes to the delivery of policies and frameworks across the UK
j) influence key decision makers
k) support research and development of the evidence base for speech and language therapy .

Why the data sharing is necessary to achieve those aims:

The processing of personal data about speech and language therapists and other individuals using the RCSLT Online Outcome Tool (ROOT) is required to ensure that the individuals accessing the ROOT have a legitimate reason for doing so. This is required to ensure the fidelity of the outcome data collected and to enable use of the system to be audited. It is also required to support users of the system, including in instances whereby help is requested.

Once the pseudo anonymised patient data is shared with the ROOT, speech and language therapy services have access to the analytics and reports on their data, supporting aims (a) – (g). The minimum amount of data about individuals receiving speech and language therapy is collected in order to achieve this.

As a by-product, the profession is developing a dataset about the outcomes of speech and language therapy. A consistent approach to data collection across the profession and the sharing of pseudonymised patient data supports benchmarking (aim 'e') and achievement of aims (h) – (k) at a national level. In order to achieve these aims, the RCSLT will share anonymised data and publish summaries of the findings with a range of audiences and partners, including the RCSLT membership, policy makers and higher education institutions. The findings will be published in a number of different formats, including policy briefings, academic publications and presentations, some of which will be made publicly available via the RCSLT website.

The benefits we hope to bring to individuals or to society more widely:

The processing of personal data about speech and language therapists is critical for this project, which is having benefits to individuals and the broader society. The profession is using the data on speech and language therapy outcomes to improve the quality of care provided to individuals receiving speech and language therapy. The data is also being used to support decisions about the planning and redesign of services, which has the potential to optimise use of resources in the NHS and other providers. The findings from the data are also being used to demonstrate the impact of speech and language therapy to key stakeholders, including policy-makers, funders and commissioners, as part of RCSLT influencing and lobbying work to ensure that the value of speech and language therapy is recognised. This is essential as part of our ongoing campaigning to improve access to SLT services for people with communication and swallowing needs in the UK.

(Examples available at: https://rcslt-root.org/Content/root-publications-resources-and-useful-links)

3. Organisations involved in the data sharing:

Name	Organisation	Responsible Person	Email address	Telephone
Jonathan Bowles	Royal College of Speech and Language Therapists	Head of Corporate Services/Data Protection Officer	dpo@rcslt.org	0207 378 3018
DPO name	**Organisation name**	Data protection officer;		
Paddy Guest	Different Class Solutions Ltd	Director/Data Protection Officer	paddy@different-class.com	0333 0888 338

In any instance where an additional organisation needs to be added to the existing data sharing agreement, this should be agreed in writing by the Data Controllers.

4. Sharing data with another controller:

When acting with another controller as joint controllers of personal data, there is a legal obligation to set out the responsibilities in a joint control arrangement, under both the UK GDPR/Part 2 of the DPA 2018 and under Part 3 of the DPA 2018.

Art. 26 GDPR Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Determination of respective responsibilities for compliance with the obligations under the Regulations:

RCSLT

- Ensures the required data processing agreement is in place
- Provides oversight of the data processor and their activities
- Handles the communication of any requests to the data processor from the other joint controllers (for example erasure of data)
- Reporting any known issues, including data breaches
- Initiating a routine review of this data sharing agreement on a biennial basis
- Ensures all its staff with access to the ROOT are aware of responsibilities in line with data protection legislation
- Responds to any subject access requests from users of the ROOT

Organisation name

- Reporting any known issues (including data breaches and loss in transit / transfer)
- Ensuring only staff with legitimate reason for accessing the ROOT are granted access to the ROOT (and with appropriate level of access) and that accounts are de-activated when no longer needed
- Ensuring all patient data is pseudonymised/de-personalised prior to sharing
- Initiating amendment to this data sharing agreement in the event that there is a change in the personal data items being shared (section 5)
- Ensures all staff with access to the ROOT are aware of responsibilities in line with data protection legislation
- Determines the appropriate retention period and ensures that the data is managed in accordance with this
- Responds to any subject access requests from patients
- Responds to requests for erasure and actioning the removal of any data prior to the usual retention period in the event that this is required
- Routinely reviews the information provided to ensure it is up to date
- Informs patients about how pseudonymised/de-personalised data about them is used (for example, in their privacy notice)

5. Personal data items being shared

In some cases it may be appropriate to attach 'permissions' to certain data items, so that only particular members of staff or staff in specific roles are allowed to access them; for example, staff who have received appropriate training.

Personal data collected about the individuals using the ROOT includes:

- Name
- Employing organisation
- Email address
- RCSLT membership number (where applicable)
- The IP address that the user connects from

Who has access?

- RCSLT staff with system administration responsibility
- Different Class Solutions Ltd staff with system administration responsibility
- Staff at **Organisation name** who have been appointed as system administrators on behalf of their organisation

The data collected about the individuals receiving speech and language therapy includes:

- A pseudonymised local patient identifier
- Gender
- Year of birth
- Medical diagnoses
- Communication and swallowing disorder descriptor(s)
- Therapy Outcome Measure (TOMs) scale
- Therapy Outcome Measure (TOMs) scores
- Date of TOMs rating
- Type of TOMs rating (start-of-episode/interim/end-of-episode/discharge):
- **Organisation to add**
- _____
- _____
- _____
- Any other patient or rating data item that may from time to time be added to the ROOT, provided that data item does not contain any personally identifiable information

Additional fields may be added locally, if required, but additional data shared with the ROOT by users of the system must comply with local information governance policies and frameworks. Additional fields that will be submitted to the ROOT are listed below:

- **Organisation to add**
- _____
- _____

This list should be reviewed each time this data sharing agreement is reviewed.

Organisation name should initiate amendment to this data sharing agreement in the event that there is a change in the personal data items being shared.

Who has access?

- RCSLT staff with system administration responsibility
- Different Class Solutions Ltd staff with system administration responsibility
- All staff at **Organisation name** with access to the ROOT

6. Lawful basis for sharing

Clearly explain your lawful basis for sharing data. The lawful basis for one organisation in a data sharing arrangement might not be the same as that for the other one.

If you are using consent as a lawful basis for disclosure, then your agreement should provide a model consent form. You should also address issues surrounding the withholding or retraction of consent.

You should also set out the legal power under which you are allowed to share the data.

	RCSLT	**Organisation name**
Personal data collected about the individuals using the ROOT	Legitimate interests	_____ _____
Pseudo-anonymised patient data	Legitimate interests	_____ _____

7. Special category data, sensitive data or criminal offence data:

You must document the relevant conditions for processing, as appropriate under the UK GDPR or the DPA 2018, if the data you are sharing contains special category data or criminal offence data under the UK GDPR, or there is sensitive processing within the meaning of Part 3 of the DPA 2018.

The personal data collected about the individuals using the ROOT does not include special category data.

The patient data does include special category (health) data, which has been pseudo-anonymised.

GDPR article 9(2)(i) permits you to process special category data if:

"processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy".

The relevant basis in UK law is set out in the DPA 2018, in Schedule 1 condition 3. In order to rely on this condition the processing must be carried out either:

- by, or under the responsibility of, a health professional; or
- by someone else who in the circumstances owes a legal duty of confidentiality.

Recital 54 of the UK GDPR gives more guidance on what is meant by 'public health':

"all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality."

You must be able to demonstrate that the processing is necessary for reasons of **public interest** in the area of public health. The term 'public interest' is not defined, but you need to point to a benefit to the wider public or society as a whole, rather than

to your own interests or the interests of the particular individual. In particular, recital 54 makes clear this condition should not enable processing for other purposes by employers, or by insurance or banking companies.

This condition may for example apply where the processing is necessary for:

- public health monitoring and statistics
- reviewing standards of clinical practice

8. Access and individual rights:

All controllers within this agreement remain responsible for compliance, even in instances where process assigns responsibility for particular tasks.

For joint controllers, Article 26 of the UK GDPR and section 58 of the DPA 2018 for Part 3 processing require you to state in the agreement which controller is the contact point for data subjects. In all instances related to patient data this agreement, the point of contact for data subjects will be **Organisation name.** This will include requests for access to shared data or other information, whether it is under the data protection legislation, or under freedom of information legislation.

In all instances related to users of the ROOT, the RCSLT will be the point of contact for the data subjects.

The DPO at each organisation takes overall responsibility for ensuring that the individual can easily gain access to all their personal data that has been shared. Details regarding patients' rights are included in the information governance pack.

9. Information governance arrangements:

In order to:

- have detailed advice about which datasets they can share, to prevent irrelevant or excessive information being disclosed, the ROOT is configured such that data can only be shared for the agreed fields.
- make sure that the data they are sharing is accurate (for example by requiring a periodic sampling exercise and data quality analysis) each organisation can routinely run reports on their data (both in aggregated form and raw form). Each user also has a dashboard displaying key statistics to enable them to continually monitor the accuracy of the data submitted to the ROOT.
- record data in the same format (abiding by open standards when applicable) the RCSLT provide a document defining each field to promote consistency. Additionally, the ROOT is built with data standards embedded.
- have common rules for the retention and deletion of shared data items, as appropriate to their nature and content, and procedures for dealing with cases where different organisations may have different statutory or professional retention or deletion rules:
    - the pseudonymised patient data may currently remain on the system for as long as the organisation wish to participate in this project. The agreement and use of the service will be reviewed every two years, at which time each

controller will reassess the basis and appropriateness for continued use of the system.

- the personal data collected about the individuals using the ROOT will be retained indefinitely for active accounts; inactive accounts will be monitored and individuals notified every 18 months.

- have common technical and organisational security arrangements, including the transmission of the data and procedures for dealing with any breach of the agreement in a timely manner; the agreements currently in place state: “notify the person named in “Notify the person named in Clause 3, immediately in instances where a data breach is identified or suspected. The UK GDPR introduces a duty to report certain personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible”.
- ensure their staff are properly trained and are aware of their responsibilities for any shared data they have access to; this is set out as part of the acceptable use policy that new users sign[i]
- have procedures for dealing with access requests, complaints or queries from members of the public; these should be directed to the RCSLT data protection officer (dpo@rcslt.org) for users of the ROOT, and to the data protection officer at **Organisation name** for patients.
- the ongoing effectiveness of the data sharing initiative and the agreement that governs it; the RCSLT currently sets a review period of two years
- have procedures for dealing with the termination of the data sharing initiative, including the deletion of shared data or its return to the organisation that supplied it originally; upon the written agreement of the Data Controllers, the agreement may be terminated at any stage. The RCSLT will be responsible for arranging the

permanent deletion of any shared data upon on termination of this Agreement, except as required by applicable law to store the Data and except for one copy that it may retain and use for a period of up to three months for back-up and audit purposes only.

10. Under what circumstances will the data be accessed?

ROOT users' data:

- Accessed by staff at RCSLT/Different Class Solutions Ltd for the purposes of administration of the system, providing technical support and audit
- Accessed by staff **Organisation name** for management of user accounts and audit

Pseudonymised patient data:

- Accessed by staff at RCSLT/Different Class Solutions Ltd for the purposes of providing technical support
- Accessed by staff at **Organisation name** to support patient care, update records, audit, analysis
- Accessed by staff at RCSLT to support analysis

11. How will the data be stored?

The data is stored on a securely hosted web system utilising SQL Server 2016 or later and ASP.net 4.8. The servers have SSL certification to ensure that all data flowing to and from the server is encrypted and could not be deciphered if intercepted in transit. The servers are protected by firewalls to protect the data and prevent unauthorised access by anyone else. The data is stored using an encryption algorithm so that if anyone physically removed a disk or the server itself, they would not be able to access the data.

The servers are located in UK data centres, on UK-only nodes. The data centres are provided by Microsoft Azure, all meeting the security standards of ISO27001.

12. How will the data be returned/destroyed?

Different Class will, at the written direction of the Data Controller(s), delete or return the Data and copies thereof to the Data Controller(s) on termination of this Agreement except as required by applicable law to store the Data and except for one copy that it may retain and use for a period of up to three months for back-up and audit purposes only.

13. Review frequency:

Every 2 years.

14. Further details (Annex)

This is a statutory code of practice made under section 121 of the Data Protection Act 2018.

The code focuses on the sharing of personal data between controllers, ie where separate or joint controllers determine the purposes and means of the processing of personal data, as defined in UK GDPR Article 4(7).

If a controller asks another party to process personal data on its behalf, for the purposes of the UK GDPR the other party is a “processor”, as defined in Article 4(8) of the UK GDPR. The UK GDPR draws a distinction between a controller sharing personal data with another controller, and a processor processing personal data on behalf of a controller.

Article 28 of the UK GDPR lays down requirements that must be in place between a controller and processor, in order to protect the rights of the data subject. These requirements include a written contract and guarantees about security. Under the UK GDPR a processor must only process personal data on documented instructions from the controller. A processor has its own liabilities and responsibilities both under the contract and the UK GDPR.

15. The agreement

By signing this document, signatories agree to data being shared and jointly controlled as set out above.

Signed for and on behalf of the RCSLT:

Name: Jonathan Bowles

Position: Head of Corporate Services / Data Protection Officer

Date: _____

Signature: _____

Signed for and on behalf of Organisation name

Name: _____

Position: _____

Date: _____

Signature: _____