## 

## 

## **DATA SHARING AGREEMENT**

## **(Controller to Controller)**

**between**

**THE UNIVERSITY OF MANCHESTER**

**and**

**[INSERT FULL LEGAL NAME OF SCHOOL]**

**DATA SHARING AGREEMENT**

between

**THE UNIVERSITY OF MANCHESTER**, a charitable body registered in England charitable body registered in England under registration number RC000797 incorporated under Royal Charter and having its main administrative offices at Oxford Road, Manchester M13 9PL ("**Manchester**")

and

**[Insert full legal name of school],** [insert full legal address of school]

Manchester and [name of school] are each a "**Party**" to this Agreement and are hereinafter referred to together as “the Parties”.

**BACKGROUND**

1. [NAME OF SCHOOL] has agreed to share specified pupil level data with Manchester as part of the Passport to Success Project.
2. In carrying out the Project, the Parties will share personal data with each other;
3. The Parties have agreed to enter into this agreement in respect of the sharing, use, storage and disposal of personal data on the terms set out below.

**TERMS AND CONDITIONS**

It is hereby agreed as follows:

# DEFINITIONS AND INTERPRETATION

## In this agreement, unless the context requires otherwise, the following words have the following meanings:

|  |  |
| --- | --- |
| **Agreement** | means this data sharing agreement, including the Schedule; |
| **Approved Countries** | means the UK and countries in the European Economic Area; |
| **Commencement Date** | means **11.11.2022** notwithstanding the date or dates of signature of this Agreement; |
| **Confidential Information** | means the Data and any other information (including samples, materials, drawings, specifications, photographs, designs, computer code, computer programs, software, data, formulae, processes, know-how, any technical or commercial information), reports, papers, correspondence or documents which is disclosed by one Party to the other, or to any of such other’s officers, employees or students, in whatever form, (including written, oral, visual or electronic), and which is, or which should reasonably be expected to be, of a confidential nature; |
| **controller, data subject, data subject request, personal data, processor, process, processed and processing** | shall have the meaning given to those terms in the applicable Data Protection Laws; |
| **Data** | means the personal data described in Part 1 (Data Processing Particulars) of the Schedule; |
| **Data Protection Laws** | means:   1. the UK GDPR, the Data Protection Act 2018, and the Privacy and Electronic Communications (EC Directive) Regulations 2003, all as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) EU Exit Regulations 2019; 2. to the extent applicable, the GDPR; 3. any other directly applicable laws or regulations relating to data protection and privacy; and 4. applicable guidance and codes of practice issued by a data protection or privacy regulator;  as amended from time to time or replaced by successor legislation, regulation, guidance or codes of practice; |
| **Data Provider** | means a Party providing Data under this Agreement as set out in Part 1 (Data) of the Schedule; |
| **Data Recipient** | means a Party receiving Data under this Agreement as set out in Part 1 (Data) of the Schedule; |
| **GDPR** | means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation); |
| **Purpose** | means the purpose set out in Part 1 (Data Processing Particulars) of the Schedule; |
| **Project Contact** | the Project contact for each Party listed in Part 3 (Notice Addresses) of the Schedule; |
| **Regulator Correspondence** | means any correspondence or communication (whether written or verbal) from a data protection or privacy regulator (in the UK, the Information Commissioner’s Office) in relation to the processing of personal data; |
| **Schedule** | means the Schedule annexed to and forming part of this Agreement; and |
| **UK GDPR** | means the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018. |

## In this agreement, unless otherwise expressly provided or unless the context requires otherwise:

### a "**person**" includes a natural person, corporate or unincorporated body (whether or not having separate legal personality);

### any words following the terms "**including**", "**include**", "**in particular**","**for example**"or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms; and

### a reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time.

# PURPOSE

## The Parties agree to share the Data for the Purpose in accordance with the terms of this Agreement.

# LAWFUL BASIS

## The Parties acknowledge and agree that:

### the legal basis for processing of personal data for the Purpose is Article 6(1)(e) UK GDPR (performance of a task in the public interest);

### the additional legal basis for processing special category personal data for the Purpose is Article 9(2)(j) UK GDPR (processing in the public interest, scientific or historical research purposes or statistical purposes).

# DATA PROCESSING PARTICULARS

## The Parties acknowledge and agree that the data processing particulars of the personal data to be processed by the Parties under this Agreement are as set out in Part 1 (Data Processing Particulars) of the Schedule.

# SEPARATE CONTROLLERS

## The Parties acknowledge and agree that each Party shall be a separate controller and shall comply with the obligations of a controller under the Data Protection Laws in respect of its use of the Data.

# FAIR PROCESSING NOTICES / Consents / APPROVAls

## Data Provider shall ensure that it is not subject to any prohibition or restriction which would:

### prevent or restrict it from disclosing or transferring the Data to Data Recipient;

### prevent or restrict it from granting Data Recipient access to the Data; or

### prevent or restrict either Party from using the Data;

### for the Purpose.

## Data Provider shall ensure that all fair processing notices, consents, and /or regulatory and ethical approvals have been given and are sufficient in scope to enable each Party to use the Data for the Purpose in accordance with the Data Protection Laws.

# PROCESSING

## Each Party shall:

### use Data solely for the Purpose;

### not make any copies of Data except as may be necessary for carrying out the Project;

### implement appropriate technical and organisational measures including the security measures set out in Part 2 (Security Requirements) o the Schedule, so as to ensure an appropriate level of security is adopted to mitigate the risks associated with the processing of Data, including against unauthorised or unlawful processing, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or damage or access to the Data;

### keep the Data confidential and not sub-license, transfer, disclose or otherwise make available Data in whole or part to any third Party except with specific prior written consent from Data Provider;

### ensure the reliability of any of its employees and students who have access to the personal data and ensure that such employees and students have committed themselves to confidentiality obligations or are under an appropriate statutory obligation of confidentiality;

### maintain a record of processing activities as required by the applicable Data Protection Laws;

### use reasonable endeavours to notify Data Provider if it is obliged to make a disclosure of any of the Data under any statutory requirement, such notification to be made in advance of such disclosure or immediately thereafter, unless prohibited by applicable law.

## Each Party shall provide the other Party with all information and assistance reasonably required to ensure and demonstrate the Parties’ compliance with the Data Protection Laws and the terms of this Agreement in relation to the processing of the Data.

# DATA SUBJECT REQUESTS AND REGULATOR CORRESPONDENCE

## Each Party undertakes that it shall:

### notify the other Party in writing within 2 working days of any data subject request or Regulator Correspondence received by it in respect of the Shared Personal Data; and

### provide a Party receiving a data subject request or Regulator Correspondence with all information and assistance reasonably required to enable the receiving Party to consider and respond to such data subject request or Regulator Correspondence in accordance with any deadline and any requirement to provide information.

# BREACH NOTIFICATION

## Each Party will promptly (and, in any event, no later than 2 working days after becoming aware of a breach concerning to the Shared Personal Data or suspected breach) inform the other Party in writing of any breach or suspected breach of any of its obligations under this Agreement and of any other unauthorised or unlawful processing, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or damage or access to the Data. Such notification shall specify (at a minimum):

### the nature of the breach or suspected breach,

### the date and time of occurrence,

### the extent of the Data and any data subjects affected or potentially affected,

### the likely consequences of any breach or suspected breach (should it have occurred) for data subjects affected by it; and

### any measures taken or proposed to be taken by the Party who has suffered the breach or suspected breach to address and remedy the breach and / or mitigate its possible adverse effects.

## The Party who has suffered the breach or suspected breach shall thereafter promptly, where requested and at the requesting Party’s expense:

### provide the requesting Party with all such information as the requesting Party requests in connection with such breach or suspected breach;

### take such steps as the requesting Party reasonably requires it to take to mitigate the detrimental effects of any such breach or suspected breach on the requesting Party; and

### otherwise cooperate with the requesting Party in investigating and dealing with such breach or suspected breach and its consequences.

# CONFIDENTIALITY

## The Party receiving or acquiring Confidential Information (the “**Receiving Party**”) from the other Party (the “**Disclosing Party**”) undertakes for so long as such Confidential Information remains confidential in character:

### to keep all such Confidential Information confidential, and to take all reasonable steps to ensure that copies of the Confidential Information made by or on behalf of the Receiving Party are protected against theft or other unauthorised access;

### not to communicate or otherwise make available any such Confidential Information to any third Party except with specific prior written consent from the Disclosing Party;

### to disclose Confidential Information only to such personnel employed by the Receiving Party who have a specific need to receive such Confidential Information for the Purpose, and who are aware and have accepted that the Confidential Information is, and should be treated as, of a confidential nature; and

### not to use, or allow to be used, Confidential Information other than solely for or in relation to carrying out the Project, unless (and then only to the extent to which) any other use shall have been specifically authorised in writing by the Disclosing Party.

## The obligations contained in this clause 11 shall survive the expiry or termination of this Agreement for any reason but shall not apply to any Confidential Information which:

### at the time of disclosure, has already been published or is otherwise in the public domain other than through breach of the terms of this Agreement;

### after disclosure, is subsequently published or comes into the public domain by means other than an action or omission on the part of the Receiving Party;

### the Receiving Party can demonstrate was known to it or subsequently independently developed by it and not acquired as a result of participation in the Project;

### was lawfully acquired from a third Party who did not obtain it from the Receiving Party;

### is required to be disclosed to any regulatory authority or court of competent jurisdiction; or

### is required to be disclosed pursuant to a request under the the Freedom of Information (Scotland) Act 2002 or Environmental Information (Scotland) Regulations 2004.

# WARRANTIES AND DISCLAIMERS

## Data Provider warrants that it is entitled to provide the Data to Data Recipient for the Purpose.

## Subject to clause 12.1, Data Recipient assumes all liability for damages that may arise from its use, storage, or disposal of the Data. Data Provider shall not be liable to Data Recipient for any loss, claim or demand suffered by Data Recipient, or made against Data Recipient by any other Party, due to or arising from the use, storage, or disposal of the Data by Data Recipient.

# LIABILITY

## Subject to clause 13.3, the liability of either Party to the other Party for any breach of this Agreement or arising in any other way out of the subject matter of this Agreement, will not extend to:

### loss of business;

### loss of profit; or

### any indirect, special, or consequential damages or losses.

## Subject to clause 13.3, the maximum aggregate liability of either Party for losses arising under or otherwise in connection with this Agreement shall not exceed £500,000.

## Nothing in this Agreement limits or excludes either Party’s liability for:

### death or personal injury resulting from negligence; or

### any fraud; or

### any other liability which, by law, cannot be limited or excluded.

# TERM AND EXPIRY

## This Agreement shall take effect from the Commencement Date and shall continue in force for so long as any of the Data is being processed by the Parties, notwithstanding completion of the Purpose or termination of any related agreements.

## The Parties shall, at the end of the relevant retention period set out in Part 1 (Data Processing Particulars) securely destroy and permanently delete Data from their systems (including back-up and archive systems).

## The provisions of clause 1 (Definitions), 11 (Breach Notification), 12 (Confidentiality), this clause 14.3, clause 15 (Notices), 16 (Dispute Resolution) and 17 (General) shall survive the expiry of this Agreement.

# NOTICES

## All notices given under this Agreement shall be in writing and, subject to clause 15.2, may be given by email to the Project Contacts.

## Any notices given under clause 16 (Dispute Resolution) shall be in writing and sent by registered or recorded delivery post to the notice addresses set out in the Schedule.

# DISPUTE RESOLUTION

## If any dispute arises out of this Agreement the Parties will first attempt to resolve the matter informally through designated senior representatives of each Party to the dispute, who are not otherwise involved with the Project. If the Parties are not able to resolve the dispute informally within a reasonable time not exceeding 2 months from the date the informal process is requested by notice in writing they will attempt to settle it by mediation in accordance with the Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure.

# GENERAL

## Neither Party may assign or sub-contract any of its rights, benefits or obligations under this Agreement without the prior written consent of the other Party.

## This Agreement constitutes the entire agreement between the Parties for sharing of the Data for the Purpose, and no statements or representations made by any Party have been relied upon by the other in entering into this Agreement.

## Any variation to this Agreement shall be in writing and signed by authorised signatories for both Parties.

## This Agreement shall be governed by, and construed in accordance with, the laws of Scotland and the Parties agree to the exclusive jurisdiction of the Scottish courts.

## This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. A signed copy of this Agreement delivered by e-mailed portable document format file or other means of electronic transmission shall be deemed to have the same legal effect as delivery of an original signed copy of this Agreement.

**IN WITNESS WHEREOF** this Agreement is executed as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| For and on behalf of **THE UNIVERSITY OF MANCHESTER:** | | | | |
| Full name: |  |  | Signed: |  |
| Title: |  |  | Date: |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| For and on behalf of **[INSERT FULL NAME OF SCHOOL]** | | | | |
| Full name: |  |  | Signed: |  |
| Title: |  |  | Date: |  |

###### Data Processing Particulars

*Data being Provided by Manchester*

Subject to external dependencies (e.g. sufficient response rate) being met, Manchester will provide aggregated PDF feedback reports on an annual basis. The outputs do not constitute sharing of individual personal data as they are based on aggregates of at least 10 pupils. Scores are not calculated for any outputs that represent fewer than 10 pupils, consistent with the Office for National Statistics’ guidance on disclosure thresholds.

*Data being Provided by [insert school name]*

The data processing particulars of the personal data shared by [insert school name] to be processed by the Parties under this Agreement are as set out below:

|  |  |
| --- | --- |
| The subject matter of the processing | Re-use of socio-demographic data items (specified below) that contain identifying personal information in addition to special category data. |
| Duration of the processing and retention period(s) | From the point of receipt until such time as identifying personal information is no longer required (e.g. all data linkage opportunities which require such information have been exhausted) - until the end of 2026 based on current external dependencies (e.g. timing of data linkage opportunities in the National Pupil Database). |
| The nature of the processing | Structuring (e.g. organising and aggregating data by school)  Storing (e.g. secure storage of project data on Isilon)  Combining (e.g. matching/linkage of data as noted above)  Erasing/destroying data (e.g. excising data in cases where pupils are opted out of the study). |
| The purpose(s) of the processing | The purposes are (a) preparation and structuring of individual pupil password lists to enable secure access to the Passport to Success survey; (b) aggregation of data to populate school feedback reports; (c) Statistical analysis of data; and, (d) further linkage of data to other sources (e.g. educational outcomes in the National Pupil Database). |
| The types of personal data processed | See table below |
| The categories of data subjects to whom the personal data relate | Pupils in Year 4 (i.e., aged 8-9) in the 22/23 school year attending primary schools participating in the Passport to Success study. |

*Data items specified in this agreement are:*

|  |  |  |
| --- | --- | --- |
| Data item | Description | Rationale |
| Unique Pupil Number (UPN) | 13-character code that identifies each pupil | UPN is required to enable future linkage to educational outcome data within the National Pupil Database (NPD), specifically, end of Key Stage 2 academic attainment outcomes.  This is consistent with the DfE’s position on the intended purpose of the UPN system (available [here](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/807381/UPN_Guide_1.2.pdf)): “to provide invaluable evidence on educational performance to inform independent research” (DfE, 2019, p.4).  The intended use of the UPN in the Passport to Success project noted above therefore serves an educational purpose, as it will enable the University to determine, for example, the extent to which the Passport programme improves educational outcomes. Moreover, one of the key overarching aims of the Passport to Success project is to inform educational provision in participating schools.  The above position is consistent with the DfE view on the use of the UPN by third parties. |
| Forename and Surname | e.g., John Doe | Forename and Surname are required in order for the University to prepare individual pupil password lists to enable secure access to the Passport to Success survey in each participating school. In addition, this information is also used in combination with UPN (see above) to enable accurate matching to educational data in the NPD. |
| Year Group | 4 (in 2022/2023) | Year Group is required in order to:  (a) check that all submitted pupil data are eligible (in other words, that only the Y4 cohort in a given school have been included), and that (b) in the case of mixed-form schools (i.e., smaller schools in which more than one Year Group are part of the same class), we are able to differentiate between pupils in the eligible year group and those in the ineligible year group. |
| Class number/name/identifier | e.g., Y4 Class 1, 2 etc, or Year 4 Acorn, Year 4 Oak etc | Class number/name/identifier is required in order that we are able to cluster pupil level data by class/teacher. This is particularly pertinent in larger schools, where there may be 2 or even 3 classes per year group. Several of our statistical analyses rely on this information. |
| Year 5 (23/24) teacher name | Name of the teacher who will be teaching the above class in 23/24, e.g. Mrs Smith | As noted above, we need to structure our pupil level data by class/teacher. The teacher’s name is required as we will also be gathering data from said teachers (see below) |
| Year 5 (23/24) teacher email address | Email address of the teacher who will be teaching the above class in 23/24, e.g. j.smith@oakdale-primary.sch.uk | As noted above, we will be gathering data from said teachers (see below) in the form of brief usual practice and outcomes surveys (all teachers), and implementation surveys (in Passport schools only). |
| Year 6 (24/25) teacher name | Name of the teacher who will be teaching the above class in 24/25, e.g. Mr Jones | As noted above, we need to structure our pupil level data by class/teacher. The teacher’s name is required as we will also be gathering data from said teachers.  **NB: these data will not be requested until spring 2024** |
| Year 6 (24/25) teacher email address | Email address of the teacher who will be teaching the above class in 24/25, e.g. j.jones@oakdale-primary.sch.uk | As noted above, we will be gathering data from said teachers in the form of brief usual practice and outcomes surveys (all teachers).  **NB: these data will not be requested until spring 2024** |
| Sex | Male, Female | Sex is required for two reasons. First, subject to response rates, sex is one of the filters used in the aggregated feedback reports used in Passport to Success (e.g., schools can view data trends by sex). Second, sex will be used as an explanatory variable in our statistical analyses of the Passport to Success survey dataset (i.e., in assessing the impact of Passport, we will control for the influence of sex on wellbeing scores and other outcomes). |
| Free School Meal eligibility | ‘EverFSM6’  Yes/No | Free School Meal (FSM) eligibility is required for two reasons. First, subject to response rates, FSM is one of the filters used in the aggregated feedback reports used in Passport to Success (e.g., schools can view data trends by FSM eligibility). Second, FSM will be used as an explanatory variable in our statistical analyses of the Passport to Success survey dataset (i.e., in assessing the impact of Passport, we will control for the influence of FSM eligibility on wellbeing scores and other outcomes). |
| Special Educational Needs provision | No SEN, Statement, EHC plan, SEN support | Special educational needs (SEN) provision is required for two reasons. First, subject to response rates, SEN is one of the filters used in the aggregated feedback reports used in Passport to Success (e.g., schools can view data trends by SEN provision). Second, SEN will be used as an explanatory variable in our statistical analyses of the Passport to Success survey dataset (i.e., in assessing the impact of Passport, we will control for the influence of SEN on wellbeing scores and other outcomes). |
| Ethnicity | Ethnicity major category data, as contained in the Department for Education’s School Census:  AOEG = Any Other Ethnic Group  ASIA = Asian  BLAC = Black  CHIN = Chinese  MIXD = Mixed  UNCL = Unclassified  WHIT = White | Ethnicity is required because it will be used as an explanatory variable in our statistical analyses of the Passport to Success survey dataset (i.e., in assessing the impact of Passport, we will control for the influence of ethnicity on wellbeing scores and other outcomes). |

###### Security Requirements

Data Provider will transfer the Data to the Data Recipient in the form of a 7-zip encrypted or password protected Excel file sent via ZendTo or email, with the access password being provided to the Data Recipient by phone and abiding by the project’s timelines. Whenever possible, files will be exchanged using ZendTo and encrypted using 7-zip or similar encryption software, with email and Excel encryption options being used as a last resort. The Data Recipient will provide a clear, step by step guide for the initial encryption and subsequent transfer process to support the above.

Data Recipient will ensure that:

the Data are only stored and processed in a secure networked environment controlled by Data Recipient\*;

where laptops are used to access the Data, the laptops have full disk encryption and are solely connected to a secure networked environment within Data Recipient’s IT infrastructure;

the Data are stored only on computer systems where access to the Data are limited by password protected individual user accounts and only authorised employees and students of Data Recipient have access to such accounts;

access to the Data are provided only to authorised employees and students of Data Recipient working on the Project;

authorised employees and students of Data Recipient with access to the Data keep passwords and usernames confidential and do not disclose or share these with any other person; and

current anti-virus and anti-malware software is installed on all systems and hardware being used to store or access the Data.

\*Full technical details of secure data storage arrangements at Manchester are as follows:

Data are to be kept in an encrypted Veracrypt container/folder (AES-256 algorithm), in a protected folder on the University's Research Data Storage system, known as Isilon.

Accessing to the data requires 2FA to log into the university's network. The folder with the Veracrypt file can only be accessed by named users, and the container is itself protected with a long password (30+ characters).

The nature of the project means that data has to be accessed frequently and elements exported on demand on a daily basis by the data manager and/or research assistants.  The above system allows for this while maintaining a very high level of security.

The encrypted container noted above is stored on an access restricted data share on the University’s network storage infrastructure which is the recommended location for storing sensitive or critical University data.  The storage infrastructure is hosted across two data centres (approx. 4KM apart) for resilience and disaster recovery purposes.   Physical access to the data centres is strictly limited to data centre staff and a limited number of authorised IT Services staff.  The data centres are protected by physical and electronic access security systems, swipe card access in and out of the data centres and CCTV coverage.  The data centres are locked down out of hours and access is discouraged, but can be arranged by prior agreement with the data centre manager.

The University’s IT Services utilises Legato Networker Backup domains. Supporting infrastructure comprises disk libraries and both physical and virtual tape libraries. Cross data centre backup is performed, so services hosted within data centre 1 (Joule House) are backed up to data centre 2 (Reynold House) and vice versa.

Backup/recovery plans are documented as part of the service install process during the commissioning of a specific service. Each Service is responsible for its business continuity and disaster recovery plans, to which IT Services feed in its technical recovery plans. ITSD operates change and release management processes. All proposed changes to infrastructure hosted, maintained and administered by IT Services are recorded via the Request for Change (RFC) process with changes being reviewed and authorised by a Change Advisory Board (CAB).

Research data storage is not backed up to tape in the traditional fashion. However, resilience is obtained through replication and use of snapshots means that files deleted by accident or corrupted can be recovered. Hourly backups can be accessed within 24 hours and daily backups can be accessed within 35 days.

###### Notice Addresses

For Manchester:

|  |  |
| --- | --- |
| Project Contact: | Dr. Joao Santos  The University of Manchester  Oxford Road  Manchester  M13 9PL  joao.santos@manchester.ac.uk |
| Legal Contact: | Director of Research and Business Engagement  The University of Manchester  2nd Floor Christie Building  Oxford Road  Manchester  M13 9PL  [contractsteam@manchester.ac.uk](mailto:contractsteam@manchester.ac.uk) |

For [name of school]:

|  |  |
| --- | --- |
| Project Contact: | [insert name and full contact details for school contact] |
| Legal Contact: | [insert name and contact details of school contact for receipt of legal notices] |