University Hospital Southampton NHS
NHS Foundation Trust

DATA SHARING AGREEMENT

Between

UNIVERSITY HOSPITAL SOUTHAMPTON NHS FOUNDATION TRUST

and

ST GEORGE CATHOLIC COLLEGE

This Agreement is dated 2021

PARTIES

(1) **UNIVERSITY HOSPITAL SOUTHAMPTON NHS FOUNDATION TRUST** of Southampton General Hospital, Tremona Road, Southampton SO16 6YD ("**UHS**")

(2) **ST GEORGE CATHOLIC COLLEGE** of Leaside Way, Southampton, SO16 3DQ ("the School")

BACKGROUND

(A) As part of HM Government's response to the COVID-19 pandemic emergency, the Department of Health and Social Care appointed UHS to establish a sub-regional COVID-19 direct RT-LAMP saliva testing hub.

(B) To enable the carrying out of the Covid-19 direct RT-LAMP saliva testing in the School, UHS and the School are required to share limited categories of personal data for the Permitted Purpose set out in this Agreement and in accordance with this Agreement.

AGREED TERMS

1 Definitions and interpretation

1.1 In this Agreement:

Complaint	means a complaint or request (other than a Data Subject Request) relating to either party's obligations under Data Protection Laws relevant to this Agreement and/or the processing of any of the Shared Personal Data, including any compensation claim from a Data Subject or any notice, investigation or other action from a Data Protection Supervisory Authority relating to the foregoing (and **Complainant** means the Data Protection Supervisory Authority, Data Subject or other person initiating or conducting a Complaint);
Controller	has the meaning given in applicable Data Protection Laws;
Data Protection Laws	means, as applicable to either party and/or to: (a) the UK GDPR; (b) the Data Protection Act 2018; (c) any laws which implement any such laws; and (d) any other applicable law relating to the processing, privacy and/or use of

Personal Data, as applicable to either party;

(e) any laws which implement any such laws; and

(f) any laws that replace, extend, re-enact, consolidate or amend any of the foregoing;

Data Protection Supervisory Authority means any regulator, authority or body responsible for administering Data Protection Laws;

Data Subject has the meaning given in applicable Data Protection Laws from time to time;

Data Subject Request means a request made by a Data Subject to exercise any right(s) of Data Subjects under Data Protection Laws in relation to any of the Shared Personal Data or concerning the processing of such data;

Disclosing Party means the Party that transfers or makes available personal or special category data to the Receiving Party for the Permitted Purpose

Permitted Lawful Basis means
for UHS

- UK GDPR Article 6(1)(e) – the processing of personal data is necessary for the performance of its official tasks carried out in the public interest in providing and managing a health service
- UK GDPR Article 9(2)(i) – the processing is necessary for reasons of public interest in the area of public health
- Data Protection Act 2018 – Schedule 1, Part 1, (2) (2) (f) – health or social care purposes
- Regulations 3(1) and (4) of the Health Service (Control of Patient Information) Regulations 2002 (COPI) – the processing is necessary for a COVID-19 purpose

For the School

- UK GDPR Article 6(1)(e) – the processing is necessary for the performance of a task carried out in the public interest.
- UK GDPR Article 9(2)(g) and Schedule 1, part 2, para 6 Data Protection Act 2018 – the processing of special category data is necessary to fulfil a statutory purpose.
- UK GDPR Article 6(1)(f) – the processing is necessary for the purposes of the

	legitimate interest of the controller. • The relevant task is set out in law, in particular in s175 of the Education Act 2002 and paragraph 3 of Schedule 1 to the Education Act 2002 for maintained schools. • Personal Data relating to staff is processed under the legitimate interest of the data controller to enable minimising the spread of COVID-19 in a timely manner and continuing the delivery of education services safely and securely and to discharge responsibilities as the employer in health and safety law.
Permitted Purpose	means direct RT-LAMP saliva testing for Covid-19 through the sub regional hub set up by UHS and confidential notification to nominated senior leadership of the School of a positive test result to initiate contact tracing to minimise the spread of the virus;
Permitted Recipients	means UHS's employees and contractors including holders of Honorary Contracts with UHS who need access to the Shared Personal Data for the Permitted Purpose and nominated senior leadership receiving confidential notification of a positive test result to initiate contact tracing to minimise the spread of the virus**;**
Personal Data	has the meaning given in applicable Data Protection Laws from time to time;
Personal Data Breach	has the meaning given in the UK GDPR;
processing	has the meaning given in applicable Data Protection Laws from time to time (and related expressions, including **process**, **processed** and **processes** shall be construed accordingly); and
Receiving Party	means the Party that receives the personal or special category transferred or made available by the Disclosing Party for the Permitted Purpose
Shared Personal Data	means Personal Data received by the Receiving Party from or on behalf of the Disclosing Party, or otherwise made available by the Disclosing Party for the Permitted Purpose.
UK GDPR	means the General Data Protection

Regulation, Regulation (EU) 2016/679, as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 and DPPEC (Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time);

2 Status of this Agreement and the parties

Each party (to the extent that it processes the Shared Personal Data pursuant to or in connection with this Agreement) shall be an independent Controller of the Shared Personal Data in its own right. Nothing in this Agreement (or the arrangements contemplated by it) is intended to construe either party as the processor of the other party or as joint controllers with one another. If the parties share the Shared Personal Data, it shall be shared and managed in accordance with the terms of this Agreement.

3 Compliance with Data Protection Laws

The Receiving Party shall at all times comply with all Data Protection Laws in connection with the exercise and performance of its respective rights and obligations under this Agreement and the processing of the Shared Personal Data. This Agreement allocates certain rights and responsibilities among the parties as enforceable contractual obligations between themselves, however nothing in this Agreement is intended to limit or exclude either party's responsibilities or liabilities under Data Protection Laws (including under Article 82 of the UK GDPR or under any similar Data Protection Laws and the duties owed by each party to Data Subjects under any Data Protection Laws).

4 Obligations on the Disclosing Party

The Disclosing Party shall ensure prior to sharing the Shared Personal Data with the Receiving Party that all appropriate privacy notices have been made available to each relevant Data Subject as necessary to permit the sharing of the Shared Personal Data with the Receiving Party for the Permitted Purpose on the Permitted Lawful Basis as envisaged under this Agreement in accordance with Data Protection Laws. During the term of this Agreement, the Disclosing Party shall promptly notify the Receiving Party if it becomes aware that a relevant Data Subject has requested that their Shared Personal Data is no longer processed by either party for the Permitted Purpose.

5 Obligations on Receiving Party

5.1 The Receiving Party shall ensure that at all times:

5.1.1 it shall undertake all processing of the Shared Personal Data only for the Permitted Purpose in accordance with this Agreement and in all respects in accordance with Data Protection Laws;

5.1.2 it shall undertake processing of the Shared Personal Data only to the extent consistent with the Permitted Lawful Basis;

5.1.3 it shall promptly (and in any event within 10 Business Days) on request provide the Disclosing Party with: (a) all copies of all notices, records and information necessary to demonstrate its compliance with this Agreement; and (b) all records referred to in paragraph 10.

6 Technical and organisational measures

6.1 The Receiving Party shall at all times:

6.1.1 put in place and maintain appropriate technical and organisational measures so as to ensure the protection of the rights of Data Subjects under Data Protection Laws and as otherwise required to meet the requirements of both parties under all Data Protection Laws; and

6.1.2 implement and maintain appropriate technical and organisational measures (which shall, at a minimum, comply with the requirements of Data Protection Laws, including Article 32 of the UK GDPR) and process the Shared Personal Data in a manner that ensures appropriate security of the Shared Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, unauthorised or unlawful destruction, loss, alteration, disclosure or access.

6.2 The Receiving Party shall at all times ensure the processing of the Shared Personal Data shall be limited to the authorised personnel of the Receiving Party or of a Permitted Recipient that:

6.2.1 need to process it for the Permitted Purpose in accordance with this Agreement;

6.2.2 are reliable and adequately trained on compliance with all Data Protection Laws and this Agreement; and

6.2.3 are subject to (and comply with) a binding written contractual obligation to keep the Shared Personal Data confidential.

6.3 The Disclosing Party shall ensure that it adopts the following security measures when transferring Shared Personal Data to the Receiving Party: provide the Shared Personal Data by encrypted Excel spreadsheet by zip file which is password protected with password being supplied separately to UHS to a nominated person or by SMS message and encrypted e-mail to a nominated person or persons at the School.

7 Disclosures to Permitted Recipients

7.1 The Receiving Party shall be liable to the Disclosing Party for all acts and omissions of each of the Permitted Recipients as if they were the acts and omissions of the Receiving Party. Each obligation in this Agreement on the Receiving Party to do, or refrain from doing anything, shall include an obligation on the Receiving Party to ensure all Permitted Recipients do, or refrain from doing, such thing.

7.2 The Receiving Party shall not engage nor permit any staff or third parties other than the Permitted Recipients to carry out any processing of any Shared Personal Data. The Receiving Party shall ensure at all times:

7.2.1 that all processing by Permitted Recipients is conducted in a manner consistent with the Permitted Lawful Basis, the Permitted Purpose, the Receiving Party's obligations

under this Agreement and the restrictions on processing imposed on the Receiving Party under this Agreement; and

7.2.2 without prejudice to the above, that each of the Permitted Recipients (other than the employees of a Permitted Recipient or the Receiving Party) carrying out any processing of the Shared Personal Data is subject to a binding written agreement regulating its processing of the Shared Personal Data which complies in all respects with the requirements of Data Protection Laws.

8 International transfers

The Receiving Party shall not transfer the Shared Personal Data to any country outside the United Kingdom or to any international organisation (as defined in the UK GDPR) without the Disclosing Party's prior written consent.

9 Data Subject Requests, Personal Data Breaches and Complaints

9.1 The Receiving Party shall promptly (and in any event within *24* hours) notify the Disclosing Party if the Receiving Party suspects or becomes aware of any actual or threatened occurrence of any Personal Data Breach in respect of any Shared Personal Data. The Receiving Party shall promptly (and in any event within *24* hours) provide all such assistance and information as the Disclosing Party requires to investigate and if appropriate, report any actual or suspected Personal Data Breach to a Data Protection Supervisory Authority and to notify affected Data Subjects under Data Protection Laws.

9.2 The Receiving Party shall promptly (and, in any event, within 5 Business Days of receipt) inform the Disclosing Party if it receives any Complaint or Data Subject Request in relation to the Shared Personal Data. When receiving and responding to a Data Subject Request or a Complaint, the Receiving Party shall consult in advance with the Disclosing Party and promptly comply with the Disclosing Party's reasonable instructions (if any).

9.3 Subject to the remainder of this Agreement, as between the parties, responsibility for compliance with and responding to:

9.3.1 any Data Subject Request relating to any Shared Personal Data falls on the party which received such Data Subject Request*;*

9.3.2 any Complaint relating to the Shared Personal Data falls on the party which receives the Complaint from a Complainant;

9.3.3 each party's respective obligations in respect of any Personal Data Breach (including notification of the Data Protection Supervisory Authority and/or Data Subject(s)) impacting or relating to any Shared Personal Data in the possession or control of the Receiving Party (or any third party with whom it has shared such data) fall on the Receiving Party; and

9.3.4 each party's respective obligations in respect of any other obligation under Data Protection Laws (including any obligation to notify the Data Protection Supervisory Authority and/or Data Subject(s) of any other Personal Data Breach) fall on each party subject to such obligation(s).

9.4 Each party shall promptly co-operate with and provide reasonable assistance, information and records to the other to assist each party with their respective compliance with Data Protection Laws and in relation to all Complaints and Data Subject Requests.

9.5 The Disclosing Party's obligations under paragraphs 9.3 and 9.4 shall be performed at the Receiving Party's expense, except to the extent that the circumstances giving rise to such obligation arose out of any breach by the Disclosing Party of its obligations under this Agreement.

10 Records

The Receiving Party shall maintain complete, accurate and up to date written records of all of its processing of the Shared Personal Data and as necessary to demonstrate its compliance with this Agreement.

11 Retention

11.1 Except as required by applicable law in the United Kingdom, the Receiving Party shall:

11.1.1 process each part of the Shared Personal Data for no longer than such processing is necessary for the Permitted Purpose (as set out in Appendix 1) and in any event cease to process each part of the Shared Personal Data on the earlier of termination or expiry of this Agreement or in the event that a data subject objects to the use of their data, unless there is a strong reason to continue processing the data that overrides the data subject's objection or if the data is being used for a legal claim; and

11.1.2 immediately, confidentially, irrecoverably and securely destroy or dispose of all Shared Personal Data (and all copies) in its possession or control that can no longer be processed in accordance with paragraph 11.1.1.

12 Miscellaneous

12.1 The provisions of this Agreement shall survive termination or expiry of this Agreement and continue indefinitely.

12.2 Any partial or total invalidity of one or more terms of this Agreement shall not affect the validity of other terms thereof.

12.3 The non-exercise or delay of the exercise of any legal or contractual right of the parties cannot be interpreted as a waiver of their right.

Appendix 1	**The Shared Personal Data**
Categories of data to be shared	Staff Member - first and last name, address, including postcode, date of birth, gender, mobile phone number, school, employee/payroll number, e-mail, saliva test results. Pupil - first and last name, address, including postcode, date of birth, gender, mobile phone number, e-mail, Unique Pupil Number, school, class and for secondary school tutor and year group, saliva test results. Parent or Guardian of Pupil - first and last name, address, including postcode, mobile phone number, e-mail.

	School contractor – first and last name, address, including postcode, date of birth, gender, mobile phone number, school, e-mail, saliva test results.
Categories of Data Subject	Participants drawn from a. School staff, b. School pupils; c. School contractors. In addition, parents/guardians will provide personal data as set out above and are data subjects
Who in Schools shares and receives the data?	HEADTEACHER Name: Mr James Habberley HEADTEACHER Email: head@stgcc.co.uk HEADTEACHER Phone Number: 02380 322603 SENIOR LEADERSHIP TEAM LINK Name: Mr Euan Douglas SENIOR LEADERSHIP TEAM LINK Email: edouglas@stgcc.co.uk SENIOR LEADERSHIP TEAM LINK Phone Number: 02380 322603 DATA MANAGER Name: Mr Neil Gulliver DATA MANAGER Email: ngulliver@stgcc.co.uk DATA MANAGER Phone Number: 02380 322603 CONTACT FOR DATA PROTECTION ENQUIRIES Email: dwalford@stgcc.co.uk
Date planned for sharing	From 3 February 2021
How will it be shared?	• By encrypted Excel spreadsheet by zip file which is password protected with password being supplied separately to UHS to a nominated person. • By SMS text and secure encrypted e-mail with password being supplied separately to School to a nominated person. • Updating of registration data will be effected by individuals through the enquiries team.
Who in UHS receives the data?	Overall supervision of Systems Team is responsibility of Professor James Batchelor, Systems Lead Programme and David Cable, Head of Digital Services. SouthamptonTesting@uhs.nhs.uk

What happens with the data when it is received?	Used for the Permitted Purpose.
What retention period shall be applied to that data?	The information processed by the NHS is kept for as long as it is required to provide the participant with direct care and to support NHS initiatives to fight COVID-19. Information held for direct care purposes are stored in line with the Records Management Code of Practice for Health and Social Care 2016. This means such information will be held for up to 8 years before it is deleted. Any personal data gathered as part of the COVID-19 direct RT-LAMP saliva testing for other purposes will be deleted at the end of the COVID-19 direct RT-LAMP saliva testing. For the avoidance of doubt, the encrypted Excel spreadsheet providing the data will be destroyed at the end of the schools testing programme and the Shared Personal Data of any person who does not or whose child does not participate in the provision of saliva samples will be deleted from the UHS database at the end of the COVID-19 direct RT-LAMP saliva testing.

SIGNED by:
GAIL BYRNE
for and on behalf of the UNIVERSITY HOSPITAL SOUTHAMPTON NHS FOUNDATION TRUST

……
Signature

Chief Nursing Office and Caldicott Guardian
……
Title

……
Date

SIGNED by
JAMES HABBERLEY
for and on behalf of ST GEORGE CATHOLIC COLLEGE

J Habberley
J Habberley (Feb 3, 2021 14:26 GMT)
……
Signature

Head Teacher
……
Title

03-Feb-2021
……
Date