Data Protection Policy

(January 2021)

Park Community School

Adopted by PCE Ltd and PCV (Charity)

The purpose of this policy is to set out how the school deals with personal information correctly and securely and in accordance with the GDPR, and other related legislation.

Document Control Table	
Associated Documents	Data Breach Policy Staff IT Policy Complaints Policy
Date Approved by governors	26/01/2021
Date of Review	January 2023

Contents

Introduction

The school collects and uses personal information (referred to in the General Data Protection Regulation (GDPR) as personal data) about staff, students, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

The school is the Data Controller, of the personal data that it collects and receives for these purposes.

The school has a Data Protection Officer, Susan Parish, who may be contacted at dpo@pcs.hants.sch.uk

The school issues Privacy Notices (also known as a Fair Processing Notices) to all pupils/parents and staff (see Appendices 1 and 2). These summarise the personal information held about students and staff, the purpose for which it is held and who it may be shared with. It also provides information about an individual's rights in respect of their personal data

Purpose

This policy sets out how the school deals with personal information correctly and securely and in accordance with the GDPR, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

What is Personal Information/data?

Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, employee/payroll number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Data Protection Principles

The GDPR establishes six principles as well as a number of additional duties that must be adhered to at all times:

1. Personal data shall be processed lawfully, fairly and in a transparent manner

2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes)

3. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive;

4. Personal data shall be accurate and where necessary, kept up to date;

5. Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

6. Personal data shall be processed in a manner that ensures appropriate security of the personal

Duties

Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA), unless that country or territory ensures an adequate level of data protection.

Data Controllers have a General Duty of accountability for personal data.

Commitment

The school is committed to maintaining the principles and duties in the GDPR at all times. Therefore, the school will:

- Inform individuals of the identity and contact details of the data controller
- Inform individuals of the contact details of the Data Protection Officer
- Inform individuals of the purposes that personal information is being collected and the basis for this
- Inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this.
- If the school plans to transfer personal data outside the EEA, the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information
- Inform individuals of their data subject rights
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point.
- Provide details of the length of time an individual's data will be kept
- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely
- Share personal information with others only when it is legally appropriate to do so
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests)
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards
- Ensure that all staff and governors are aware of and understand these policies and procedures.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years. The policy review will be undertaken by the Data Protection Officer, Headteacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact the Data Protection Officer, who may be contacted at dpo@pcs.hants.sch.uk

Appendix 1 – Park Community School Privacy Notice: For those engaged to work or volunteer at the school

This document explains how we use school workforce information

The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, previous names, employee or teacher number, national insurance number)
- addresses and contact numbers including next of kin
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught) and including pre-employment checks
- relevant medical information
- payroll information, e.g. bank details
- car insurance information [to establish adequate insurance for business purposes]
- DBS (Disclosure and Barring Service) check certificate number and disclosure date

Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid
- ensure safeguarding of students

The lawful basis on which we process this information

The lawful basis for collecting and using workforce information for general purposes includes, for example:

For personal data:

- performance of a contract with the data subject (member of staff)
- compliance with a legal obligation and/or protection of vital interests e.g. for DBS checks and maintenance of the Single Central Register for student safeguarding.
- performance of public interest tasks, includes educating students on behalf of the Department for Education (DfE) and would therefore include performance management and continuing professional development (CPD) information [note that this, for example, would also come under 'performance of a contract']
- the use of CCTV is also covered by performance of public interest tasks.
- consent would normally only apply to staff photographs/images if used for marketing purposes and to staff business cards.

For special category data (sensitive personal data, including, for example, biometric data):

- necessary and authorised by law for employment obligations

- protect vital interest where consent not feasible
- necessary for establishing, exercising or defence of legal rights
- Substantial public interest
- Explicit consent

  (See Article 6 for personal data and Article 9 for special category data from the GDPR-from 25 May 2018) as well as the Education Act 1996 – this information can be found in the guide documents on the following website https://www.gov.uk/education/data-collection-and-censuses-for-schools

Collecting this information
Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information
We hold school workforce data indefinitely in accordance with Local Authority latest current guidelines.

Who we share this information with
We routinely share this information with:

- our local authority (LA)
- the Department for Education (DfE)

Covid-19 Saliva Testing in School
In order to suppress the spread of Covid-19 we see testing being of great value to reduce the transmission. Park Community School has been asked to be part of trial Saliva testing programme provided by University Hospital Southampton NHS Foundation Trust (UHS).

Data will need to be shared with UHS and permission will be sought from students, staff and contractors.

Data will be collected under the General Data Protection Regulations:

- Article 6(1)(e) – the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Article 9(2)(g) – the processing is necessary for reasons of substantial public interest.

Please see Appendix 5 Data Protection Impact Assessment and Appendix 6 Data Sharing Agreement for more information.

For staff member data shared will be, name, address, date of birth, gender, mobile phone number, school, email.

Contractor to school who registers for testing, first and last name, address, date of birth, gender, mobile phone number, company and personal email.

Positive test results of the above.

Why we share school workforce information
We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority
We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)
We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding/expenditure and the assessment of educational attainment.

We are required to share information about our school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements
The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools, and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the DfE including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The DfE may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The DfE has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether the DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the DfE's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact dpo@pcs.hants.sch.uk (the Data Protection Officer – Susan Parish, and the data team)

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the data protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information
If you would like to discuss anything in this privacy notice, please contact:
Susan Parish, Data Protection Officer

Appendix 2 - Park Community School Privacy Notice for Parents and Students

This document explains how we use our students' personal information.

Why do we collect and use personal information?

We collect and use personal information:

- To support pupil learning (including with GDPR compliant providers of external online web applications e.g. MyEd, MILK, MyMaths and Educake)
- To monitor and report on pupil progress
- To provide appropriate pastoral care and career guidance
- To assess the quality of our services and how well our school is doing
- For statistical forecasting and planning
- To comply with the law regarding data sharing

The categories of personal information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address, parent email address and telephone number, emergency contact)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons) and exclusions
- Assessment information
- Modes of travel
- Relevant medical information
- Special educational needs information
- Exclusions / behavioural information
- Post 16 learning information (e.g. destination)
- Looked after child (LAC) status
- Pupil premium status

The General Data Protection Regulation allows us to collect and use pupil information on the following basis: with consent of the individual/parent, where we are complying with a legal requirement, where processing is necessary to protect the vital interests of an individual or another person and where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

When the personal information is Special Category Information we may rely on processing being in the substantial public interest in addition to consent of the individual/parent and the vital interests of the individual or another.

Our requirement for this data and our legal basis for processing this data includes the Education Act 1996, 2002 and 2011, The Childrens Act 1989 and 2004, Education and Skills Act 2008, Schools Standards and Framework Act 1998 and the Equalities Act 2010. (See also Article 6 for Personal Data and Article 9 for Special Category Data from the GCPD May 25th 2018)

Most of the personal information you provide to us is mandatory. For example: names, contact details, relevant medical information, special educational needs, attendance information, free school meal eligibility and photographs for use on our management information system (MIS.) Information is also passed on to us from previous schools, including, for example: assessment, attendance and behaviour data. However, some information provided to us is done so on a voluntary basis. To comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain personal information to us or if you have a choice in this. This is done through the Park Community School Parental Consent Policy Document, available in hardcopy from reception and online on the MyEd Ap. Information for which we need your consent includes, for example: biometric data, the taking of students' images for publication e.g. on the school's website and trips where information will need to be passed onto an external company. Where we are using your personal information only on the basis of your consent you may ask us to stop processing this personal information at any time.

Storing personal data
We keep information about students and their parents on computer systems and sometimes on paper.

We hold education records securely and retain them in accordance with the Retention Schedule after which they are destroyed.

Who do we share pupil information with?
We routinely share pupil information with:

- Schools/colleges
- Our local authority (including social services, court and police)
- The Department for Education (DfE)
- NHS (e.g. CAHMS)

Aged 14+ qualifications
For pupils enrolling for post 14 qualifications, the Learning Records Service will give us a pupil's unique learner number (ULN) and may also give us details about the pupil's learning or qualifications

Covid-19 Saliva Testing in School
In order to suppress the spread of Covid-19 we see testing being of great value to reduce the transmission. Park Community School (PCS) has been asked to be part of trial Saliva testing programme provided by University Hospital Southampton NHS Foundation Trust (UHS).

Data will need to be shared with UHS and permission will be sought from students and parents. The student data will be used to protect student welfare and carry out safeguarding activities.

Data will be collected under the General Data Protection Regulations:
- Article 6(1)(e) – the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

- Article 9(2)(g) – the processing is necessary for reasons of substantial public interest.

Please see Appendix 5 Data Protection Impact Assessment and Appendix 6 Data Sharing Agreement.

For students the data we hold as a school regarding name, address, date of birth, gender, mobile phone number, school, class and tutor group will be shared.

For parent/carer of student: name, address, mobile number and email.

Positive test results of the above.

Why we share pupil information
We do not share personal information with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:
To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services

What is different about pupils aged 13+?
Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent / guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

The National Pupil Database (NPD)
The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on

educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, parents and pupils have the right to request

access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact [setting to include contact details of their administrator / Data Protection Officer]

You also have the right, subject to some limitations to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact:
If you would like to discuss anything in this privacy notice, please contact:

dpo@pcs.hants.sch.uk (The Data Protection Officer and team)

Appendix 3 – Park Community School Privacy Notice for Clients

- Park Community Services
- Park Community Enterprises Ltd (PCE)
- Park Community Ventures
- Park Community Catering

We are committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR). It applies to all clients to whom we provide paid services.

Park Community School is a "data controller" for all the organisations listed above. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information. We may amend this notice at any time.

Data protection principles
We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

The kind of information we hold about you
Personal data, or personal information, means any information about an individual from which that person can be identified.

We will collect, store, and use the following categories of personal information about you where applicable:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses, qualifications and public liability insurance cover, membership details and constitutions of organisations.
- Name of child if appropriate e.g. for party bookings
- Bank account details
- CCTV footage

The legal basis for holding this information
The legal basis for holding this information is that it is necessary for us to fulfil the contract we have with you when you are purchasing a service from us and where processing is necessary for the performance of a task carried out in the public

interest or in the exercise of official authority vested in the controller. Where the data is used by us to market products or services to you then we will require your consent (see paragraph below.)

How is your personal information collected?
We collect personal information about your service requirements through Community booking form, PCE order form, club constitutions, certificates and telephone orders, emails and verbally.

How we will use information about you
We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you
2. Where we need to comply with a legal obligation
3. Where it is necessary for our legitimate interests (or those of a third party, for example auditors or our insurance companies) and your interests and fundamental rights do not override those interests

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests)
2. Where it is needed in the public interest or for official purposes

If you fail to provide personal information
If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers.)

Change of purpose
We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Consent
We would like to be able to keep you up to date with marketing information such as new services that become available and offers that we may wish to make available to you. For this we would need your consent. This is obtained by your completion of the consent section on the booking form / initial enquiry form.

You have the right to withdraw this consent in writing at any time, through emailing pdp@pcs.hants.sch.uk and/or bookings@pcs.sch.uk

Data sharing
We may have to share your data with third parties, including third-party service providers, where required by law, where it is necessary to administer the working

relationship with you or where we have another legitimate interest in doing so. This might include for example auditors or our insurance company or the police. In each case your interests and fundamental rights do not override those interests.

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies and the law. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Security
We have appropriate security measures in place to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention
We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Rights of access, correction, erasure, and restriction
It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Under certain circumstances, by law you have the right to:
- Request access to your personal information (commonly known as a "data subject access request")
- Request correction of the personal information that we hold about you
- Request erasure of your personal information
- Object to processing of your personal information
- Request the restriction of processing of your personal information
- Request the transfer of your personal information to another party

Contact
For further information about your rights, or if you have any questions about this privacy notice or how we handle your personal information, please contact pdp@pcs.hants.sch.uk and/or bookings@pcs.sch.uk

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Appendix 4 – Park Community School Privacy Notice for Job Applicants

This Privacy Statement is published by Park Community School.

By submitting your application or your CV, you acknowledge having read and understood this Privacy Statement. If you do not wish your information to be used as follows, please do not submit your application or your CV.

This Privacy Statement sets out:
- which personal data we gather in the course of the application and recruiting process;
- how we use your personal data;
- who has access to your personal data;
- how long we keep your personal data;
- how you can access and modify the personal data we collect about you;
- how we secure your personal data;
- how you can submit questions and remarks.

Which personal data do we collect?
This Privacy Statement relates to all personal data that we receive from you and that we collect and process about you in the context of your application and the resulting recruitment process.

These personal data include: identification and contact details, personal characteristics (such as gender and date of birth), education and work experience (including results, certificates, degrees, references), job preferences, financial data (e.g. current and desired salary), all data in your CV and cover letter, all publicly available data from your LinkedIn profile and other social media or public websites, and all other personal data you have provided to us orally or in writing in the context of your application.

How do we use your personal data?
Your personal data will be used in the context of your application and recruitment process, including for:
1. evaluating your skills, qualifications and interests against our career opportunities;
2. checking your data, your references and/or conducting background checks (where applicable);
3. communication concerning the recruitment process and your application;
4. implementing improvements to the organisations' application and recruitment process
5. The processing for the purposes 1, 2 and 3 described above are necessary for a potential employment contract and the processing for purpose 4 is based on the legitimate interest of the organisation to improve its processes on the basis of your application and recruitment procedure.

Who has access to your personal data?
Your personal data can be shared with [Company name] and if needed with other affiliates of [company name]. Within these entities, the following staff members have access to your data:
- staff members of the HR department;

- recruiting manager;
- senior management

In certain cases, technical staff members may have access to your personal data, but only insofar this is necessary to ensure the proper functioning of our technical systems.

The organisation may make use of external service providers or third parties for any of the purposes described above (e.g. recruitment websites or agencies conducting background checks). In such case, access to your personal data will be limited to the purposes described in this Privacy Statement, and in accordance with the requirements of the applicable data protection legislation.

How long do we retain your personal data?
If your application is not successful, we will retain your personal data for a maximum period of 6 months unless we have your explicit consent to hold it for longer.

If your application is successful, your personal data obtained in the context of the application and recruitment procedure will be included your personnel file. You will then be informed separately of how the organisation processes personal data of personnel.

Appendix 5 – Data Protection Impact Assessment for Saliva Testing

Data sharing in the context of the School's participation in the COVID-19 Saliva Testing in Schools

Data Protection Impact Assessment	
Name of controller	Park Community School
Contact	Susan Parish
Effective date	25 January 2021

1. Summary of the Project and why we are carrying out a DPIA

This DPIA considers risks to the rights and freedoms of individuals whose personal data will be shared by Park Community School (the '**School**') with University Hospital Southampton NHS Foundation Trust (**UHS**) in the context of the joint initiative between the Department of Health and Social Care, UHS and the NHS more broadly, Southampton City Council and University of Southampton to undertake COVID-19 testing.

This cooperation is undertaken with the aim to suppress the spread of COVID-19 in schools and other educational establishments and through that, to promote and safeguard the welfare of the pupils and the members of the school community and to enable all children to have the best outcomes. The School sees its participation in testing as the opportunity to make COVID-19 testing available to its pupils and staff, which is of great value given the national crisis around the testing and widespread difficulties with timely access to COVID-19 tests at the moment.

To enable the carrying out of the COVID-19 saliva testing at the School, the School is required to share limited categories of personal data of its pupils (including pupils' parents' or carers' contact details) and staff with UHS/the NHS.

Taking the COVID-19 saliva test by pupils and staff is voluntary and the participants express their consent by submitting their saliva samples.

We do not consider the proposed sharing of the personal data to be likely to result in a high risk to the rights and freedoms of pupils, their parents or carers or staff. It is in this context that we do not consider this DPIA to be mandatory under Article 35 of the GDPR. However, motivated by the intention to uphold the best practice and the highest standards of accountability in relation to the personal data that the School processes, we have decided to carry out this DPIA, to document the relevant risks and the measures that we have implemented to mitigate them.

2. The processing

2.1 The context of the data sharing

2.1.1 The data subjects are pupils, their parents or guardians and staff at Park Community School. The data shared will therefore include

personal data of groups considered to be vulnerable, such as children. The categories of personal data to be shared will include:

- pupil personal data- first and last name, address, including postcode, date of birth, gender, mobile phone number, school, class and for secondary school tutor and year group;
- parent or guardian of pupil - first and last name, address, including postcode, mobile phone number, e-mail;
- staff member - first and last name, address, including postcode, date of birth, gender, mobile phone number, school, e-mail;
- contractor to School who registers for testing - first and last name, address, including postcode, date of birth, gender, mobile phone number, company and person e-mail;
- positive test results of the above.

2.1.2 The School has not previously shared the relevant personal data with UHS/the NHS in the same way as is proposed. This is because the proposed sharing of personal data has only become necessary in the context of COVID-19 pandemic. Although there is an element of novelty in relation to this sharing of personal data, data subjects affected would generally expect their data to be shared with the NHS in some circumstances.

2.1.3 To ensure that the proposed data sharing is carried out transparently and that the affected data subjects retain control over their personal data, the School will:

(i) communicate with parents and to staff, describing the school's participation in the COVID-19 testing and the way that the school will share personal data with UHS/the NHS to enable the testing at schools (please see Data Protection Policy – January 2021 and the Data Sharing Agreement between the University Hospital Southampton NHS Foundation Trust);

(ii) circulate to parents and to staff a joint privacy notice (please see the joint privacy notice attached);

(iii) amend both its staff and pupil privacy notices to reflect the proposed data sharing and will draw parents' and staff's attention to the updated privacy notice in the communication referred to above;

(iv) include the information about the right to object to the processing in the letter to parents and to staff and also in the relevant privacy notices;

(v) will make the relevant staff aware of how to handle any potential objections and queries from data subjects; and

(vi) address the issue of dealing with data subjects' objections and requests in a data sharing agreement between the School and UHS.

2.1.4 The School has also considered the current state of technology in this area and has selected a method of transfer of the data sets that will meet the requirements of data protection law, including Article 32 of GDPR (transferring an encrypted file, with the password being

supplied separately to UHS to a nominated person).

2.1.5 The School will enter into a data sharing agreement with UHS (the '**Data Sharing Agreement**').

2.1.6 The School is aware that the processing of personal data in the context of COVID-19 pandemic attracts public attention, including concerns. We have ensured that only the minimum amount of personal data necessary to achieve the purpose will be shared between the School and UHS/NHS, that the data sharing, necessary for the performance of the School's public task, will be lawful, fair and proportionate and that the individuals affected will know that they have the opportunity to object.

2.2 **The purposes of the data sharing**

2.2.1 The School has decided to take part in the COVID-19 testing with the objective of suppressing the spread of COVID-19 at the School (and to assist with the potential roll out of a broader testing programme in further schools). The School intends to facilitate the carrying out of COVID-19 saliva testing at the School to promote and safeguard the welfare of the pupils and the members of the school community, including their health and to avoid closing down of the School due to a potential spread of COVID-19. The School believes that its participation in the COVID-19 testing will enable children to have the best outcomes (health-wise and education-wise). The sharing of personal data is necessary to enable the NHS to deploy test kits to pupils and staff at the School, which will support the participation by all those individuals who are interested but may otherwise not be able to take part in the testing due to various logistic difficulties.

2.2.2 The proposed data sharing as a part of the School's participation in the Programme will therefore benefit those individuals whose data will be shared and will have broad benefits for the pupils and staff at the School. It may also assist with a roll-out of the Programme nationally, resulting in benefits for pupils and school communities at other schools in protecting them from the consequences of the COVID-19 pandemic.

2.3 **The nature and scope of the processing**

2.3.1 The categories of personal data to be shared have been set out in 2.1.1 above. Only those categories of personal data that are necessary to enable the carrying out of the testing in the School, will be included in the data sharing.

2.3.2 The data will be transferred from the School to UHS and vice versa using a method of transfer that meets the requirements of data protection law, including Article 32 of GDPR (transferring an encrypted file, with the password being supplied separately to UHS to a nominated person and by SMS text and secure encrypted e-mail

with password being supplied separately to School to a nominated person).

2.3.3 The way that personal data will be used under the Data Sharing Agreement will be restricted to only use this data for the purpose of the COVID-19 testing, which safeguards and promotes the welfare of children who are pupils at the School.

2.3.4 The Data Sharing Agreement prevents UHS from transferring shared personal data outside the United Kingdom without the School's consent and it requires that UHS deletes the shared personal data at the end of the COVID-19 testing.

3. Lawfulness, necessity and proportionality of the processing - compliance measures

3.1 The lawful basis for processing

The School has carefully considered potential lawful bases for the governing bodies of the schools to be able to share the data of the data subjects with UHS for the purpose of the Programme. The School relies on

- Article 6 (1)(e) of the GDPR, as the proposed sharing of personal data is necessary for the performance of a task carried out by the School in the public interest.
- 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.
- GDPR Article 6(1)(f) – the processing is necessary for the purposes of the legitimate interest of the controller.

The School can use education legislation to support processing personal data for COVID-19 testing and the relevant task is to safeguard and promote the wellbeing of pupils for processing personal data for COVID-19. The legislation which underpins this is:

FOR MAINTAINED SCHOOLS
s175 of the Education Act 2002, which states as follows:

The governing body of a maintained school shall make arrangements for ensuring that their functions relating to the conduct of the school are exercised with a view to safeguarding and promoting the welfare of children who are pupils at the school.

PART 3
Welfare, health and safety of pupils
6. The standards about the welfare, health and safety of pupils at the school are those contained in this Part.
7. The standard in this paragraph is met if the proprietor ensures that—
(a) arrangements are made to safeguard and promote the welfare of pupils at the school; and
(b) such arrangements have regard to any guidance issued by the Secretary of State.

Ancillary to the above is the governing bodies' requirement to have regard to the statutory guidance Keeping Children Safe in Education (2020) ("Guidance"). The Guidance is issued under s175 of the Education Act 2002, and defines safeguarding and protecting the welfare of pupils as:

- protecting children from maltreatment;
- preventing impairment of children's physical health or development;
- ensuring children grow up in circumstances consistent with the provision of safe and effective care; and
- taking action to enable all children to have the best outcomes.

The governing bodies are seeking to ensure that the children's physical health is not impaired, through providing them with access to free COVID-19 tests. In addition, this action is going to assist in keeping schools open, enabling children to have fewer interruptions to their education and therefore enabling children to have the best outcomes.

Supporting the above is also s10 of the Children Act 2004. This requires the local authority to promote co-operation between the authority and 'relevant partners' to improve the well-being of pupils in the local authority's area (the Schools is a relevant partner in this regard). The governing body's facilitating the sharing of the data as required is a manifestation of the School's co-operation with the local authority in order to improve the well-being of its pupils at the school (i.e. in the authority area).

To enable the COVID-19 saliva testing to commence at the School, the School has to undertake certain steps, including the sharing of personal data. The sharing of the personal data is necessary to allow the pupils and staff members to take part in a testing scheme at the School, which will assist in identifying and suppressing COVID-19 infection, and therefore will both safeguard and promote the welfare of those pupils. In allowing the conduct to proceed, the governing bodies are discharging their functions in a way that safeguards and promotes the welfare of the pupils and in particular will benefit the more vulnerable pupils.

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.

The lawful basis relied on by the School for this sharing of personal data has been discussed with Information Commissioner's Office to ensure that the School has a robust lawful basis for the intended processing.

3.2 The sharing of personal data achieves the intended purpose (safeguarding and promoting the welfare of children who are pupils at the School) and, given the scale of the testing, the logistic, time constraints and the fact that the infection rate has been increasing sharply, there is no other feasible way to achieve the same outcome, i.e. enable the COVID-19 saliva testing to take place at the School promptly.

3.3 The proposed data sharing will comply with the principle of data minimisation (see paragraphs 2.1.1 and 2.3) and the Data Sharing Agreement mitigates the risk of the data being used by UHS or the School for purposes other than those necessary for the COVID-19 saliva testing.

3.4 The individuals have been provided with comprehensive information about the intended sharing of their data with UHS and vice versa and have been informed about their rights, including the right to object (see para 2.1.3).

3.5 The Data Sharing Agreement includes provisions intended to safeguard and support data subjects' rights, including their right to object.

3.6 No processors will be involved in the data sharing and pursuant to the Data Sharing Agreement, the data will not be processed outside the United Kingdom without the School's consent.

4. Assessment of risks and measures to mitigate risks

4.1 Identified risks

	Description	**Condition for approval**	**Level of residual risks to data subjects' rights**
1.	The School needs to have lawful basis for the intended sharing of personal data	Lawful basis established – see paragraph 3.1	Low
2.	Data sharing needs to be carried out transparently and fairly in a way that respects data subjects' rights, e.g. gives individuals the right to object.	(i) Transparency requirements have been satisfied through communications with parents/carers and staff and through the provision of an updated privacy policy – see paragraph 2.1.3. (ii) The School has given the individuals as much time to object prior to the sharing of the data, as is reasonably possible, given the tight timescales of the proposed COVID-19 testing and balanced against the objectives of the data sharing exercise. (iii) The Data Sharing Agreement includes provisions intended to safeguard and support data subjects' rights, including their right to object, following the sharing of the personal data.	Low

3.	Loss of control by individual data subjects over their personal data	(i)The School has taken the steps to ensure that the individuals are aware of the data sharing (see paragraph 2.1.3) and can exercise their right to object (as above). (ii)The Data Sharing Agreement expressly provides that UHS may not process the shared personal data for the purposes of communicating with individuals who have not consented to take part in the Programme without the consent of the Headteacher at the School.	Low
4.	Personal data being used in a way that data subjects would not normally expect	(i) The School has taken the steps to ensure that the individuals are aware of the data sharing and can exercise their right to object (as above) (ii) The Data Sharing Agreement contractually limits the scope of permitted use by UHS and vice versa. Ultimately, given that UHS will become an independent controller of the shared personal data, the School will not be able to retain control over the use of this data by UHS, but by entering into the Data Sharing Agreement the School has taken steps available to it to ensure that that data will be processed lawfully, fairly and securely.	Low/Medium
5.	Risk of a data breach during transfer	The School has considered security measures adequate for this transfer – see paragraph 2.1.4	Low/Medium

6. Sign off

Item	Name/position/date	Notes
Measures approved by:	Christopher Anders, Headteacher 25 January 2021	
Residual risks approved by:		
DPO advice provided:		
Summary of DPO advice:		
DPO advice accepted or overruled by:	INSERT DETAILS	If overruled, you must explain your reasons
Comments:		
This DPIA will kept under review by:	INSERT DETAILS	The DPO should also review ongoing compliance with DPIA

Appendix 6 – Copy of Data Sharing Agreement between UHS and Park Community School for Saliva Testing

DATA SHARING AGREEMENT

Between

UNIVERSITY HOSPITAL SOUTHAMPTON NHS FOUNDATION TRUST

and

PARK COMMUNITY SCHOOL

This Agreement is dated 2021

PARTIES

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

(2) **Park Community School** of [Middle Park Way, Havant, Hampshire PO9 4BU] ("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 GDPR; (b) the Data Protection Act 2018; (c) the Directive 2002/58/EC (ePrivacy Directive) and/or the Privacy and Electronic Communications (EC Directive) Regulations 2003; (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 Chapter III of the GDPR or under any similar 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
GDPR	means the General Data Protection Regulation, Regulation (EU) 2016/679;
Permitted Lawful Basis	means For UHS • 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 • 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 • GDPR Article 6(1)(e) – the processing is necessary for the performance of a task carried out in the public interest. • 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. • GDPR Article 6(1)(f) – the processing is necessary for the purposes of the legitimate interest of the controller. • For Maintained Schools - The relevant task is set out in law, in particular in s175 of the Education Act 2002.] • 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.

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 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.

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 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 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 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, 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.
Who in Schools shares and receives the data?	Christopher Anders, Headteacher Ella Capaldi, Head of School Jamie Bryce, Assistant Headteacher Phil Warren, IT Network Manager
Date planned for sharing	From 25 January 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 Christopher Anders for and on behalf of Park Community School

……
Signature

Head Teacher
……
Title

25 January 2021
……
Date