“COVID-19 Lateral Flow Testing (test and trace)”

*Data Protection Impact Assessment*

Organisation Name/Data Controller Name: Craven PRS/Carol Robertson

Date final DPIA issued 29/01/2021

**REF 01**

**Project Brief and Go Live Date: 29.01.2021**

This project is to establish a process for testing asymptomatic staff and pupils.

* Routine testing will be completed once a week
* Serial testing will commence if a pupil is in contact with another person who has tested positive (testing every day for 7 days)

Pupils must opt in to the programme for testing (parent/guardian permission is sought as required). Permission must be obtained separately for both routine and serial testing.

If a pupil tests positive they must obtain a PCR test and feed the results back to the school.

The benefit of this programme will be to contain the spread of COVID-19 within the school.

A DPIA is necessary as the school will be performing tests and collecting new medical details regarding the pupil (positive/negative COVID-19 status).

For More information provided by the DfE:

 

**Project Manager/Owner:**

|  |  |
| --- | --- |
| Name: | **C Robertson** |
| Job Title: | **Headteacher** |
| Service: | **Craven Pupil Referral Service** |
| Telephone: | **01756630495** |
| Email: | **c.robertson@cravenprs.org** |

**Information Asset Owner/s:**

|  |  |  |
| --- | --- | --- |
| Name: | **C Robertson** |  |
| Job Title: | **Headteacher** |  |
| Service: | **Craven Pupil Referral Service** |  |
| Telephone: | **01756630495** |  |
| Email: | **c.robertson@cravenprs.org** |  |

**System Administrator/ICT Contact (if applicable):**

|  |  |
| --- | --- |
| Name: | **Schools ICT/Richard Freytag** |
| Job Title: | **ICT Technician** |
| Service: | **North Yorkshire Schools ICT** |
| Telephone: | **01756630495** |
| Email: |  |

Part One – Information Flow

*The collection, use and deletion of personal information should be described here.*

PCR test is completed and results provided to the school by the parent/data subject. This is recorded in Bromcom.

DHSC share this information with the NHS, PHE, GP and local government

If a pupil has tested positive information is shared with:

DHSC via test and trace system

Test results are stored in a spreadsheet updated by the school and input into the NHS test and trace system

Test results are destroyed after 14 days

If the pupil tested positive results are shared with parent/guardian

The data subject completes a test and details are recorded.

Part Two – Privacy Risks questionnaire

* *This should be filled out during consultation between the Project Officer(s) and Data Protection Officer.*
* *Risks should be associated with the Principles of the General Data Protection Regulation (GDPR).*
* *You only need to consider risks arising from any new procedures and/or solutions.*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Privacy Issue** | **Comments** | | | | | | | **Is there a risk?**  **Address in Part Three** |
| 1. ***General*** | | | | | | | | |
| Have you identified the Information Asset Owner? | *C Robertson Headteacher* | | |  | | | |  |
| How many individuals will be affected by this project? | *18* | | |  | | | |  |
| Who are the Data Subjects? | Staff and Pupils | | |  | | | |  |
| Please select any information that will be processed: | **Personal Identifiers/information** | | | | | **Special Category** | |  |
|  | Name | | | |  | Sex life |
|  | Address/Postcode | | | |  | Sexual Orientation |
|  | Date of Birth | | | |  | Religion |
|  | Telephone Number/Email | | | |  | Philosophical belief |
|  | Emergency contact details | | | |  | Political opinion |
|  | National Insurance Number | | | |  | Trade Union Membership |
|  | NHS Number | | | |  | Ethnic Origin |
|  | Gender | | | |  | Medical history details |
|  | Images (photo/film) | | | |  | Physical health information |
|  | Pseudonymised information | | | |  | Mental health information |
|  | IP addresses | | | |  | Genetic/Biometric (eg. Thumbprint) |
|  |  | Other (please state): Unique identifier for the test  Parent/guardian details | | | |  |  |  |
| How will the personal data be collected? | Directly from the Individual | | | | | | |  |
| School MIS Records | | | | | | |
| Does this processing include data matching, automated decision making or profiling? (please describe) | N/A | | | | | | |  |
| 1. ***Lawfulness, Fairness, and Transparent*** | | | | | | | | |
| What is the lawful basis for processing personal information? If you are using more than one condition please specify which condition relates to specific data.  *(Please speak with your DPO about this)* | e) Public Task (specify) | | | | Choose an item. | | |  |
| * to safeguard and promote the welfare of pupils and children under the * Maintained Schools: Education Act 2002 for maintained schools (Section 175). This will not prevent the individual being asked for permission for the test to be carried out. However once the test has been conducted the processing of the personal data will fall under the above. | | | | | | |
| If Legitimate Interests/Public Interest Assessment (see guidance), is completed please add: | | | | | | |
| If you are processing Special Category Information (highlighted in red above), what is the lawful basis for processing this information *(Please speak with your DPO about this)* | i) Public health (check condition 3 in guidance) | | | | Choose an item. | | |  |
| Basis in law and schedule condition:  This data is processed under the obligations set out in Public Health legislation (Regulations 3(1) and (4) of the Health Service (Control of Patient Information) Regulations 2002 (COPI)) which allows the sharing of data for COVID related purposes and where it is carried out by a health care professional OR someone who owes an equivalent duty of confidentiality to that data. | | | | | | |
| Please refer to the guidance | | | | | | |
| If you are using consent how are you collecting this and how will people be able to withdraw their consent? | N/A – permission will be collected to carry out the test, but consent will not be relied on to process the resulting personal data. | | | | | | |  |
| How will you tell people about this processing? | Privacy Notice, provided by the DfE – Test and Trace app | | | | | | |  |
| Do you need to update your privacy notices? |  | | Yes | | | | |  |
|  | | No | | | | |
| 1. ***Purpose Limitation*** | | | | | | | | |
| Are you going to use information you already hold about individuals for a purpose it is not currently used for? |  | | Yes, please specify why it is currently held and under which legal basis: | | | | |  |
|  | | No | | | | |
| Have you identified all of the purposes for which you will use personal information? |  | | Yes | | | | |  |
|  | | No. If no, why not? | | | | |
| Will people expect their information to be processed in this way? |  | | Yes – once permission has been given to conduct the test, it is within reasonable expectations that the resulting personal data will be processed in this way. | | | | |  |
|  | | No | | | | |
| 1. ***Data Minimisation*** | | | | | | | | |
| How will you ensure you are only collecting information that is relevant to this specific purpose? | There is a set amount of information necessary to ensure that testing can be completed and adequate information provided to the DHSC for testing purposes. We will not collect any additional information to this. | | | | | | |  |
| Have you considered what information you could disregard |  | | Yes, please detail if any has been removed: | | | | |  |
|  | | No | | | | |
| 1. ***Accuracy*** | | | | | | | | |
| How are you going to ensure that the personal information will be kept accurate and up to date? | Routine testing is completed twice every week.  Test results are dated and deleted after 14 days. | | | | | | |  |
| How are you going to ensure that the quality of the data you collect is sufficient for your intended purpose? | We are following guidelines, staff have been trained and reminders to maintain 14 day timescales are on the calendar. | | | | | | |  |
| If you are procuring a new system does it allow you to amend and / or delete information when necessary?  *(Consult IT as necessary)* |  | | Yes | | | | |  |
|  | | No, please give details: we are working on our usual internal network and via the testing portal | | | | |
|  | | Notes can be added to the system where accuracy is disputed | | | | |
|  | | N/A | | | | |
| 1. ***Storage Limitation / Records Management*** | | | | | | | | |
| How long will the information be kept for? (retention period) | 14 days from completed test. | | | | | | |  |
| Are you procuring a system that will allow you to delete information in line with your retention periods?  *(Consult IT as necessary)* |  | | Yes | | | | |  |
|  | | No, if no why not?  Manual deletion on School Test Register | | | | |
|  | | N/A | | | | |
| What method will be used, to securely destroy paper and/or electronic records? (*Consult IT/processor as necessary)* | Deletion of file via O365 recycle bin emptied on completion of testing. R Freytag to delete recycle bin and C Robertson to delete original file off O365 Admin Sharepoint | | | | | | |  |
| Will destruction be certificated or added to a destruction log?  *Please respond.* |  | | Yes, please specify: Destruction log | | | | |  |
|  | | No, if no why not? | | | | |
| Where will information be stored/accessed? | Cloud based application | | | | | | |  |
| Other (specify): O365 | | | | | | |
| If you are using a ‘Cloud Based’ system to store or transfer information, where is the geographical location of the server/s? *(you may need to ask your provider to supply this)* | The transfer of information is done using:   * Amazon Web Services (AWS) which hosts the central system (cloud server) that supports the app * The Health Informatics Service (THIS), which is hosted by the Calderdale and Huddersfield NHS Foundation Trust. THIS provides the ‘NPEx’ system which provides test results to the app (using the test code unique to the app) * Microsoft's UK Datacentres Durham, London, and Cardiff | | | | | | |  |
| If back up information is stored off-site, where is the geographical location? | Redstor - Berkshire | | | | | | |  |
| 1. ***Security*** | | | | | | | | |
| Who will have access to the information within the organisation? | Roles: Trained staff | | | | | | |  |
| What controls have been put in place to limit access to the information? | All staff have access to Pupil data via our MIS and confidentiality contracts are already in place | | | | | | |  |
| If you are implementing a new system, does this system have the ability to audit access (audit trails)? |  | Yes | | | | | |  |
|  | No | | | | | |
|  | N/A | | | | | |
| Does your new system/hardware/procedure provide adequate protection against security risks? Please detail.  *(Consult IT as necessary)* | *e.g. encryption, two factor authentication, lockable/fire proof storage/updated policies*  *All data in O365 is encrypted.* | | | | | | |  |
| Are staff undertaking any additional training to help use new systems/procedures? Will this include Data Protection training? |  | Yes (please give details) Training on how to access portals have been given and certified via DfE training. Staff had GDPR update refresher 05/01/2021 | | | | | |  |
|  | No. If no why not? | | | | | |
|  |  |  | | | | | |  |
| Is there a disaster recovery plan in place in case of equipment/software failure? *(you may need to ask your provider to supply this)* |  | Yes | | | | | |  |
|  | No | | | | | |
| 1. ***Data Processors – Data Processors should be listed after part 2 of this form*** | | | | | | | | |
| If you are using a data processor, how has the provider demonstrated an adequate level of information security? *(you may need to ask your provider to supply this)* | **N/A** | | | | | | |  |
| If using a data processor, how has the provider demonstrated that they are compliant with GDPR? *(you may need to ask your provider to supply this)* | **N/A** | | | | | | |  |
| If using a data processor, do you have a written contract in place with GDPR clauses? |  | Yes (please attach) | | | | | |  |
|  | No | | | | | |
|  | N/A | | | | | |
| 1. ***Information Sharing – Data Controllers should be listed after part 2 of this form*** | | | | | | | | |
| What is the legal basis for sharing?  *(Please speak with your DPO about this)* | This data is processed under the obligations set out in Public Health legislation (Regulations 3(1) and (4) of the Health Service (Control of Patient Information) Regulations 2002 (COPI)) which allows the sharing of data for COVID related purposes and where it is carried out by a health care professional OR someone who owes an equivalent duty of confidentiality to that data. | | | | | | |  |
| Is there a sharing agreement in place?  *(Please speak with your DPO about this)* |  | Yes (please attach) | | | | | |  |
|  | No. | | | | | |
|  | N/A | | | | | |
| Will you transfer information outside of the UK, where will this be? |  | Yes, please specify where: | | | | | |  |
|  | No | | | | | |
|  | N/A | | | | | |
| How will information be transferred? | *e.g. email, post, secure file transfer*  *Secure Government portal* | | | | | | |  |
| ***10. Rights of the Data Subject*** | | | | | | | | |
| How will you manage ‘Subject Access Requests’ or other requests regarding information rights?  *(Rectification, erasure, objection, and restriction etc.)* | Following existing SAR protocols | | | | | | |  |
| If procuring a new system, will this allow you to fulfil the rights of the data subject mentioned above? |  | Yes, detail as needed: | | | | | |  |
|  | No | | | | | |
| If the project involves automated decision making do you have a process in place to facilitate human intervention? Please detail. | N/A | | | | | | |  |
| Will your data processing exclude individuals from using a service or from exercising any rights? |  | Yes, detail as needed: | | | | | |  |
|  | No | | | | | |
| ***11. Accountability*** | | | | | | | | |
| As a result of this project do you need to update any of the following? |  | Information Asset Register (Veritau provide a template for this) | | | | | |  |
|  | Policies | | | | | |
|  | Procedures | | | | | |
| If needed, have you consulted relevant stakeholders/ICO? What was the outcome? |  | Yes, who? please add outcome details:  Parents and Staff consent in place. Privacy notices issued | | | | | |  |
|  | No | | | | | |

**List any Data Controllers information will be shared with (if applicable):**

|  |  |
| --- | --- |
| **Name:** | The Local Authority |
| **Name:** | Department of Health and Social Care (DHSC) |
| **Name:** | National Health Service (NHS) |
| **Name:** | Public Health England (PHE) |
| **Name:** | Pupil’s GP |

**List any Data Processors information will be processed by (if applicable):**

|  |  |
| --- | --- |
| **Name:** |  |
| **Contact Details:** |  |
| **Name:** |  |
| **Contact Details:** |  |
| **Name:** |  |
| **Contact Details:** |  |
| **Name:** |  |
| **Contact Details:** |  |

Part Three – Risk Evaluation

|  |  |  |
| --- | --- | --- |
| **Privacy Risks (from part two)**  Describe source of risk and potential impact on individuals, compliance and school risks | **Options to reduce or eliminate risk** | **Evaluation**  Is the risk eliminated, reduced or accepted? |
| Subjects/Parents/Guardians are not aware of collection, their rights or that information is shared with other data controllers – particularly that pupils are set up with an account that is linked to the NHS test and trace app. | The DfE privacy notice will be provided. Veritau will make this clear. Parents are provided this information when medical consent is obtained – this should make the process clear and offer parents medical consent opt out, which would mean no sharing would take place. | Reduced |
| This information is not recorded on the Information Asset Register. The school is therefore not fulfilling their Article 30 GDPR (Records of Processing) obligations. | Information Asset Register will be updated. Veritau’s template may be adapted for this purpose. | Eliminated. |
| Special category data is being collected which may cause harm to individuals if disclosed to peers in the school community. | The school will take adequate security measures to prevent unauthorised disclosure or data breaches No further risk than existing data. | Accepted |
| There is no formal sharing agreement in place between data controllers. | The other Data Controllers are trusted partners and have provided information publically on their security and lawful basis for collection.  [NHS COVID-19 app: data protection impact assessment - GOV.UK (www.gov.uk)](https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-data-protection-impact-assessment)  [NHS COVID-19 app: privacy notice - GOV.UK (www.gov.uk)](https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-test-and-trace-app-early-adopter-trial-august-2020-privacy-notice) | Accepted |

Part Four – Signatures and Review

*This Data Protection Impact Assessment (DPIA) should be signed by the relevant Information Asset Owner. Should any risks be ‘accepted’ then consideration should be given to the school’s Senior Information Risk Owner (SIRO) countersigning the DPIA if this is not the individual who has completed the DPIA. All DPIAs should be approved by the Data Protection Officer.*

**Information Asset Owner**

Name: Carol Robertson

Job Title: Headteacher

Date: 28/01/2021

Signature:

**Data Protection Officer**

Name: Carol Robertson

Job Title: Headteacher

Date: 28/01/2021

Signature:

**Senior Officer (if applicable)**

Name:

Job Title:

Date: Click or tap to enter a date.

Signature:

**REVIEW DATE: 28/01/2022 (Recommend annually)**