



DPIA – Intrahealth School Vaccination Programme

Name of School/Trust	Chinley Primary School
Document Prepared by	Data Protection Officer and Peter Lambert
Reviewed by DPO	Yes- Claire Archibald
Date of DPO review	
Governor minute number/reviewed by SLT	
Governor/SLT review Date	

Version History			
Version	Date	Detail	Author
1.0	31/8/23	Master Template	Claire Archibald, Data Protection Officer
1.1	26/04/24	Updated following 2024 DPA release from IntraHealth - new documents attached in Appendix A	V Garton, Data Protection Officer

DPO Advice note:

Based on the information available at the time of writing and the checks made on the provider's documentation the DPO is satisfied that this DPIA addresses the main data protection risks of participating in this scheme. The school should ensure that the mitigation actions set out in the risk table below are carried out by the appropriate member of staff.

This DPIA should be completed by the school, who should complete any yellow highlighted areas. There should be no need to change any of the other text, but schools are free to change text where needed. The DPIA does not need to be sent back to the DPO again for review.

Introduction

Immunisation means both receiving a vaccine and then becoming immune to a disease. A full dose of vaccination generally provides immunity similar to that provided by the natural infection, but without the risk of the disease or its complications. When children and young people receive all the vaccinations included in the National routine childhood immunisation programme, this has a direct positive impact on their health and wellbeing, as well as their communities.

Achieving high levels of immunity against vaccine preventable diseases is vital to reduce the spread of infection and prevent outbreaks. High levels of immunity can result in herd immunity, whereby the protection from immunisation programmes extends to individuals who cannot be vaccinated for a number of reasons.

Evidence shows that delivering immunisations in schools reduces health disparities by making access to vaccines easier for all, for example parents don't need to take time off work to book immunisation appointments and children who are not registered with a GP are included.

Education and childcare settings have a vital role to play to support the routine immunisation programme through sharing of information with parents and caregivers at key points and by participating in the School Age Immunisation Service (SAIS). This involves sharing personal data of parents and children directly with the SAIS team.

SAIS providers are commissioned by NHS England (NHSE) to deliver the school-based immunisation programmes. The SAIS provider is contractually and legally responsible for the school-based immunisation programmes. There are several school-based immunisation programmes whose success depends on close working relationships between the schools, school nurses and SAIS providers.

The school supports the immunisation programme by hosting the SAIS team and helping them with aspects of the vaccination process, including:

- providing space and time in the timetable for vaccination
- reminding staff, children, and young people about the date of the immunisation session(s) and the need to provide consent for vaccination to be administered
- sharing information leaflets and consent forms with parents or carers
- providing a list of eligible children and young people to the SAIS team.

The school has been asked to share personal data with Intrahealth, who have won a contract to provide the SAIS scheme to schools. Sharing personal data with Intrahealth is new for the school. Intrahealth have requested that the school enter into a Data Processing Agreement. The school is therefore carrying out a DPIA to examine any data protection risks of the data sharing and to evidence that the school has carried out obligations in respect of high-risk processing.

Describe the nature, scope and context of the data processing**Whose data will be collected?**

Children's and parents/carers personal data will be collected as set out in the table below. Not all of this will be provided by the school, some of it will be provided by parents/carers who complete consent forms. Data provided by the school is marked with *.

Types of data	Yes	No	Types of data	Yes	No
Name	X*		Sex life or sexual orientation		
Date of Birth	X*		Looked after status/ previously in care		
Address	X		Health Data	X	
National Curriculum year group	X*		Race		
Contact telephone number	X		Ethnic origin		
Gender	X		Political opinions		
Profiling/analytical/insights information/cookies			Religious or philosophical beliefs		
Photograph/film footage			Trade Union membership		
Banking details			Genetic data		
Card payment information			Biometric data (where this is used for identification purposes)		
Salary/employment benefit details			Criminal Offence data		
Vulnerable adult data			Free School Meals status (including FSM6)		
Children's data	X*		SEN status/support		
Pupil UPN			Other NHS number GP name and practice code School attended	X	

How will the data be collected?

- Intrahealth will contact the school and request a class list for children in the relevant year/age group.
- School will send this list back to Intrahealth. This list will be sent back via the school's preferred method. DPO advice is that if the school does not have another preferred suitable method of sending this data securely (e.g. Egress), then this data can be sent back via email **if the attachment is password protected and the password is given back to Intrahealth using another method** (e.g. phone call). School must double check the email address is correct before sending. **Schools are free to discuss with their Intrahealth advisor which is the most suitable and secure way for this information to be delivered to Intrahealth- which could include an Intrahealth staff member collecting the information in person from the school if necessary.**
- Intrahealth will also send the school an 'e-consent' weblink and request that the school forward this link to parents using their usual communication method/platform.
- Parents will then complete the e-consent form.
- Depending on the uptake of the e-consent form, Intrahealth will then continue to update the school with information relating to which children they have vaccination consent responses for. This may mean that the class list and response information may be sent back to the school on several occasions- particularly if uptake has been low and Intrahealth need to do more work to ensure parents engage with the process.
- Intrahealth will also provide paper consent forms with children's names on it to the school for the school to forward to parents that continue to not respond to the e-consent process.

- The day before the vaccination date, Intrahealth prepare a final list of children and consent information. This is shared with the school on the day of the vaccination so they can arrange for the right children to be sent to the vaccination area.

What is the lawful basis of the processing of this data?

The lawful basis for the school processing this data is:

UK GDPR Article 6. 1. (e) 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.

[Unlikely that the school will share special category data- but if they do need to (for instance if they need to tell the Intrahealth team about a particular child need) the relevant lawful basis is UK GDPR Article 9. 2 (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

Data Protection Act 2018 Schedule 1 Condition:

Public health

3. This condition is met if the processing—

(a) is necessary for reasons of public interest in the area of public health, and

(b) is carried out—

(i) by or under the responsibility of a health professional, or

(ii) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.]

Who is data controller and processor?

The school is a data controller. In respect of information provided by the school to Intrahealth, Intrahealth act as a data processor. Separate to the information provided by the school, Intrahealth collects data on medical problems and allergies through consent forms that are completed by parents- Intrahealth acts as data controller for that task. Any information regarding vaccinations that are completed is retained by Intrahealth as a data controller.

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Yes- information will now be shared with an external commercial organisation.

How long is the data kept for?

The school will retain data in line with their normal data retention policy. As part of this DPIA the retention period for any data processed will be considered against that policy. Data that is shared with Intrahealth (where Intrahealth acts as processor for the school) is retained in line with the Data Processing Agreement.

How and where will the data be stored?

Data is stored by Intrahealth on their systems.

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? If yes, please describe the new purpose below.

No.

Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

No.

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?

No.

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.

Yes, information processed relates to children, their contact details and any health needs. Children are identified as 'vulnerable' data subjects, requiring an enhanced level of protection under data protection laws.

Note regarding Consultation

The school will consult with the Data Protection Officer and Governors. The school will inform parents that personal data will be shared with Intrahealth to facilitate the School Immunisation Programme.

Identify the privacy and related risks and mitigations

Data Protection Principle	Description and mitigation in place	Further mitigation actions that must be carried out by the school	Person responsible and if applicable, date of completion
Lawfulness, fairness and transparency.	The lawful basis for the sharing of data is Public Interest/Substantial Public Interest as set out above.	None	n/a
	The processing is fair- sharing personal data in this way is fair (and expected).	Ensure parents/carers are aware that they are being required to share data with Intrahealth- this can be done when the e-consent link is sent out using the school communication process.	Marion McCabe
	Data subjects have a right to be informed- the processing will be transparent if the school ensures that the relevant Privacy Notices are updated to include information relating to this processing activity.	Ensure relevant Privacy Notice(s) are updated.	Peter Lambert
	Data Subjects must be able to exercise their rights under data protection laws. The rights are already available to data subjects and are explained in the privacy notices- these rights are extended to the data shared/processed for this project.	Ensure that the privacy notices are up-to-date and easily available for data subjects (e.g. on school website)	Peter Lambert
Purpose limitation.	Personal data will be shared for the purpose of this processing activity- the school will not use the personal data for any other purpose beyond what it already does or reasonably needs to in pursuance of the aims stated in this DPIA. The external provider has confirmed that personal data will only be used for this purpose and no other.	None- School relies on external providers documentation giving assurances regarding the processing of personal data for this purpose only.	n/a
Data minimisation.	Personal data shared is as set out in the screening questions above. The School and the external provider deem these data sets as the	None	n/a

	minimum needed for the purpose of processing.		
Accuracy.	The school is responsible for ensuring personal data is accurate and up to date. All staff have a responsibility to ensure that data is factually correct.	Nominate member of staff responsible for ensuring personal data is regularly checked for accuracy- e.g. if a child changes personal details or joins or leaves the school during the consent gathering process.	Marion McCabe
Storage limitation.	Storage of this data is already addressed as part of school retention policies. Following expiration or termination of the Data Processing Agreement, Intrahealth will delete or return to the school all personal data except to the extent Intrahealth is required by applicable law to retain some or all of the personal data (in which case they will archive the data and implement reasonable measures to prevent any further processing). The terms of the DPA will continue to apply to such Personal Data.	Ensure staff member deletes or destroys data no longer needed- whether stored on external services or internal systems.	Peter Lambert
Integrity and confidentiality (security)	There is a medium risk that this processing could result in a data breach that either staff at the school, or the external provider could be responsible for. The impact of such a data breach would potentially be very high as the data relates to children who are vulnerable data subjects. Examples of risks: *Motivated intruders may try to hack systems to access personal data *Staff may accidentally share personal data with the wrong person *Personal data may be accidentally or maliciously deleted *The processor may not have appropriate measures in place to safeguard the personal data.	Ensure all school staff comply with instructions and guidance regarding data protection and IT usage. Regularly train staff in data protection and cyber security. Staff error is the main reason for data breach when sharing data externally- DPO regularly trains staff, but school leadership should also regularly remind and support staff to ensure that they process personal data with care and attention. When sending the class lists via email, school staff must carry out careful checks to ensure that the email is addressed correctly, that the attachment is correct and	Peter Lambert

	A Data Processing Agreement is necessary for this project. The law states that this document should contain key terms. This document has been checked by the Data Protection Officer and by school staff. The school is not in a position to carry out due diligence into the suitability of Intrahealth. NHS commissioning groups have awarded Intrahealth the contract and the school were not part of any procurement or due diligence processes. The school is responsible for ensuring their staff comply with Data Protection requirements. Intrahealth is also responsible to the school under the terms of the Data Processing Agreement and directly accountable to data subjects.	that it is password protected (with the password provided via an alternative method). Cyber-attacks are another high risk to schools- it is important that staff follow guidance and instruction given to them to minimise the risk of cyber-attack.	
Accountability.	All parties have responsibilities to account for their data protection practices. This DPIA and the documents referred/linked to in this document form part of the accountability practices of the school.	Retain evidence of work done to comply with Data Protection laws. Add this new processing activity/supplier to the Information Asset Register (RoPA) (in the Suppliers Tab of GDPRiS). This is a new process for the school and risks are not yet fully known. Often, it is not until new processes are underway that risks can be fully understood. Therefore, it is important to keep this DPIA under review over time as understanding of the risks and the way that data is processed will change in the future.	Peter Lambert

		DPO to review this DPIA and check that the school have completed it correctly.	Data Protection Officer
--	--	--	-------------------------

Risk Rating Decision

As a result of the privacy risks and mitigations it has been evaluated that the overall level of residual risk to privacy after the mitigation actions have been carried is low. The school leadership and governance should note this risk and if appropriate, include it in the Information Risks section of the School Risk Register.

Risk Register Advice Note

It is good practice for schools to have risk registers. Risk is an inherent part of school practices and it is important that risk management is part of governance and leadership. Academy trusts in particular **must** maintain a risk register, see

<https://www.gov.uk/government/publications/academy-trust-financial-management-good-practice-guides/academy-trust-risk-management> for more information.

In addition, the Information Commissioner's Office (ICO) recommends that information (data protection and IT security) risks are managed using a risk register. The ICO provides guidance in the form of a good practice study as part of their investigation into data protection compliance in Multi Academy Trusts https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618610/mats-outcome-report-v1_1.pdf (page 6)

Appendix A: Evidence of due diligence

As the Data Controller, the school may only rely on an external provider if it provides sufficient guarantees in relation to appropriate controls and GDPR compliance. The statements at the weblinks below have been checked by the School and the Data Protection Officer:

External Provider Name and Address	IntraHealth Limited 1st Floor, William Brown Centre, Manor Way, Peterlee, County Durham SR8 5TW
External Provider ICO Number	Z4936321
Contract/Data Sharing Agreement	 MASTER COMPREHENSIVE_ C
Terms of Use	
Any additional information	 Email to Schools from IntraHealth 17_L 2024  Intrahealth Letter to schools - Nottingham 2023