Data Protection Impact Assessment (DPIA)

What are Data Protection Impact Assessments?

Data Protection Impact Assessments (DPIAs) are structured assessments of the potential impact on privacy for high risk processes, and help us to identify the most effective way to comply with data protection obligations. The DPIA should form part of the overall risk assessment of the process or project.

A DPIA helps us to:

- Anticipate and address the likely impacts
- Identify privacy risks to individuals
- Foresee problems and negotiate solutions
- Avoid unnecessary costs
- Protect the organisation's reputation
- Offer assurance to stakeholders
- Meet legal requirements

The DPIA process is not only a legal requirement, but is also an important tool to help you identify and minimise the data protection risks of a project that involves processing personal data.

The DPIA process is relevant to initiatives involving the use of personal data and is particularly important when a new business process or technology initiative involves the collection, recording, sharing or retention of personal data.

The DPIA enables privacy and data protection considerations to be made in the early stages of a project, where any identified problems can be easier to resolve, rather than late or retrospective considerations where solutions can be costlier or delay implementation. A DPIA can also identify whether the project should be continued, when balanced with the rights and interests of persons affected.

The DPIA process will consider privacy in the way individual's personal data is used. This can involve privacy about: the integrity of the individual, the person, their personal information, their personal behaviour and their personal communications.

Data Protection Impact Assessment

Who is responsible for carrying out a DPIA?

The responsibility for conducting a Data Protection Impact Assessment (DPIA) lies with the Information Asset Owner (IAO) for a project and is produced as part of the project proposal. The IAO will often be the Project Manager/Lead. When a new project/initiative involving the processing of personal information is being considered, the IAO should contact the Data Protection Officer (DPO) to discuss the proposal. At this stage it may be identified that it is necessary to undertake a DPIA.

The DPIA itself should be completed by somebody who is associated with the business area of the processing activity and who has a good understanding of what the processing will involve. It is unlikely that a DPIA can be completed by one person and is likely to involve a number of stakeholders, for example IT.

It is not the DPO's responsibility to complete the DPIA, as they will not have enough knowledge of the data processing activity. The role of i-west is to advise and monitor the DPIA and to sign it off when it is complete.

Review

The DPIA should be reviewed annually, or wherever the system or method of handling used changes. This may be a significant change to a computer system or a change of policy or legislation.

What is high risk?

A high risk is considered to exist when particularly sensitive personal data is processed, a large volume is held, CCTV is in place, or any factor exists where personal data may be breached. High risk can result from a high probability of some harm, or a lower probability of serious harm.

Particularly sensitive data or 'special category data' includes:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life; or
- sexual orientation

There are separate and specific safeguards for criminal offence data, but they should also be included, for example where processed by HR.

If a high risk is identified that you cannot mitigate, you must consult the Information Commissioner before starting the processing. The ICO will give written advice within eight weeks, or 14 weeks in complex cases. I-west can advise you on this.

There is a legal requirement to consult with the DPO regarding the completed DPIA. If the service is unable to identify a control measure to bring the residual risk to an acceptable level, there is also a statutory obligation to consult with the Information Commissioner's Office.

Data Protection Impact Assessment

Project information			
Project name	Insight assessment data tracking	**Document version no.**	1
Author(s)	Sarah Savage	**Version date**	16.3.22
Information asset owner	Assessment Leads in The Partnership Trust	**Project manager (if different)**	

Version no.	Version date	Summary of key changes
1	**18.3.22**	

Do I need to complete a DPIA?	Y/N
Will the project involve the collection of new information about individuals?	N
Will the project compel individuals to provide information about them?	N
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Y
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	N
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	N
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 particularly private.	N
Will the project require you to contact individuals in ways which they may find intrusive?	N

If you have answered “Yes” to any of the above questions, a DPIA needs to be completed.

Data Protection Impact Assessment

1. Outline of the project, objectives and benefits

What does the project aim to achieve, including what the benefits will be to the organisation, to individuals and to other parties?
If this is not a new process, but a change to an existing, please describe the proposed changes.

The project involves setting up a 60-day free trial to use Insight data tracking software to store and analyse pupils' assessment data.
The main objective is for School staff (including Headteachers, Assessment Leaders, Teachers) and Central Trust staff (Director of School Improvement) to be able to access and analyse pupil, group and cohort-level data on attainment and progress with ease.
Reports will be generated to demonstrate current attainment and progress over time. Priority groups and pupils can be identified quickly to target interventions appropriately.
Historic data will be imported into Insight from other systems already used in schools (e.g. SIMS, FFT)

2. Describe the intended use of personal data

a) Describe the nature of the processing

The nature of the processing is what you plan to do with the personal data. This should include:

- How you collect the data
- How you store the data
- How you use the data
- Who has access to the data
- Who you will and/or may share the data with
- Whether you use any data processors
- Retention period(s)
- Security measures
- Whether there will be any profiling (fully automated decision-making)
- Whether you are using any new technologies
- Whether you are using any novel types of processing

Initially, existing data will be imported from SIMS and/or FFT. Insight will run updates daily, drawing down any new information which has been added to SIMS (e.g. new pupils)

New assessment data will be added by teachers/leaders directly into Insight software.

Only school leaders/teachers and the Trust's Director of School Improvement will have access to the data.

Insight's Privacy Notice states that they will not share this data with any other party.

Data will be used to generate reports for internal use by leaders to demonstrate academic achievement. Anonymised cohort data may be presented to the schools' governors and/or the Trust Standards Board 3 times per year.

Insight will retain the data for 30 days after the agreement terminates.

Data Protection Impact Assessment

b) Describe the scope of the processing

The scope of the processing is what the processing covers. This should include:

- The nature of the personal data
- The volume and variety of the personal data
- The sensitivity of the personal data
- The extent and frequency of the processing
- The duration of the processing
- The estimated number of the data subjects involved
- The geographical area covered

Pupil records include the following data:

- Unique Pupil Number (UPN)
- Legal first & last names
- Preferred first & last names
- Date of birth
- Gender
- Date pupil joined the school
- Date pupil left the school

The following data can optionally be recorded as well:

- Address – Not needed
- Ethnicity
- EAL status
- FSM history
- SEN history
- Service child status
- In-care status
- Attendance summaries
- Customer-defined groups
- Customer-defined notes and files

The number of pupils will vary per school

Most schools are likely to enter new assessment data 3 times per year and run reports at the same time. They will undoubtedly interact with the software more regularly.

c) Describe the context of the processing

The context of the processing is the wider picture, including internal and external factors which might affect expectations or impact. This might include, for example:

- The source of the data
- The nature of your relationship with the individuals
- The extent to which individuals have control over their data
- The extent to which individuals are likely to expect the processing
- Whether they include children or other vulnerable people
- Any previous experience of this type of processing
- Any relevant advances in technology or security

- Any current issues of public concern
- Whether you have considered and complied with any relevant Codes of Practice

All schools currently use equivalent systems to process assessment data. (SIMs/FFT)

All data relates to primary aged pupils in our schools. All assessments relate to teacher assessment judgements in subjects such as Reading, Writing and Maths or test results in similar areas of the curriculum.

Pupils' dates of birth, SEND/Disadvantaged status will be stored with the attainment data.

d) Describe the purposes of the processing

The purpose of the processing is the reason why you want to process the personal data. This should include:

- Statutory requirement
- Your legitimate interests, where relevant
- The intended outcome for individuals
- The expected benefits for you or for society as a whole
- The impact on the organisation if we don't do it

Schools have a statutory responsibility to report assessment data to parents and in certain year groups (Rec, Y1, Y2, Y4 and Y6) some of this data also has to be shared with DfE.

Intended outcomes: quick and easy access to data analysis over time, tracking test outcomes, attainment and progress.

Benefits: time saved in analysing complex data through this simple-to-use system.

Data Protection Impact Assessment

3. Data protection compliance

Principle 1: Use of personal data is fair, lawful and transparent

This section makes reference to Articles 6, 9 and 10 of GDPR, to demonstrate the lawful basis for carrying out the activity. If in any doubt, please consult your DPO i-west@bathnes.gov.uk

(a) We are relying on the following Article 6 basis for the processing of personal data: (delete lines that don't apply)

Necessary for the performance of a task carried out in the public interest, or in the exercise of our official authority

(b) We are relying on the following Article 9 basis for the processing special category data: (delete lines that don't apply)

Necessary for reasons of substantial interest

DPA-18 Schedule 1 Part 2 – (8) Equality of opportunity or treatment and
DPA-18 Schedule 1 Part 2 – (16) Support for individuals with a particular disability or medical condition

(c) We are relying on the following Article 10 basis for the processing of information relating to criminal convictions or offences: (delete lines that don't apply)

n/a

(d) Explain how individuals will be made aware of the processing

Schools will update Privacy Notices to include reference to the use of Insight as a data storage platform and communicate this with parents.

(e) If your service is subject to the Human Rights Act:

- Will your actions interfere with the right to privacy under Article 8?
- Have you identified the social need and aims of the project?
- Are your actions a necessary and proportionate response to the social need?

Principle 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

(a) If collecting personal data for primary use, explain how you have targeted only the information required

New assessment data is recorded in schools at least 3 times per year to track pupils' academic progress for school improvement purposes. All other personal data is held by the school when pupils join.

(b) If you are reusing personal data for further use, explain how this secondary use is compatible with the original reason it was collected.

Statutory data is shared with DfE at key points in the year in line with national reporting expectations. (EYFS, Y1 Phonics, Y2 Phonics, Y2 Teacher Assessment, Y4 MTC, Y6 SATs)

Principle 3: Use of personal data is adequate, relevant and no more than necessary

Explain how the amount of personal data you intend to use is enough to be understood by the audience but no more than the minimum needed to achieve your purpose

Schools will only use personal data which is relevant to analysis of performance, for example, to identify any significant differences between the performance of groups (e.g. gender, SEND, PPG etc) This is no different to data which would be known and used by class teachers and leaders in their day-to-day practice in the classroom. Personal data which has no relevance to academic performance, such as home address, will not be stored or processed.

Principle 4: Personal data must be accurate and kept up to date

(a) Explain how accurate recording of data will be achieved and how it will be kept up to date, where necessary

Any changes to personal data are made by school administrators into SIMs as soon as they are known. Personal data will be uploaded directly into Insight from SIMS on a daily basis (overnight).

(b) Explain any mechanisms that will allow you to amend or append data that is found to be inaccurate

If any inaccuracies are identified through analysis, these will be corrected at source in SIMs to allow Insight data to be accurate too.

Principle 5: Personal data must be kept in an identifiable format for no longer than is necessary

(a) **Data held in the new IT System:** explain how any automated and / or manual capability to delete data will be used to comply with the corporate retention schedule

Data will be held in Insight for the duration set out in The Partnership Trust's Retention Schedule (until the child leaves the school) At this point, personal data will be passed on to the next school (middle, junior, secondary, as appropriate)

(b) **Data held in an unstructured manner (paper, word / excel files etc):** explain how you will use any automated and / or manual capability to delete data in line with the corporate retention schedule

All data will be held in Insight and therefore structured.

(c) Explain how automatic destruction of individual records can be frozen on request

If these needs to be done then an instruction will be sent to Insight

Data Protection Impact Assessment

Principle 6: Personal data must be protected against unauthorised / unlawful use, accidental loss, damage or destruction

(a) Explain any technical security measures that will be put in place to protect the data

Insight is a web-based application, accessible only over a secure (HTTPS) connection. This ensures all data is encrypted while in transit.

Equin Limited (who own Insight) have achieved Cyber Essentials Plus certification. Data is hosted in Amazon Web Services (AWS) in London, UK. Amazon maintain multiple certifications for its data centres, including ISO 27001 compliance, PCI Certification, and SOC reports. Their reports can be found on the AWS Compliance website and you can read more about the specifics of their approach at https://aws.amazon.com/security/.

The school will not include any sensitive data in emails that are sent to Insight – for example for support/problems. Only pupil UPN will be used if specific identification is required.

Passwords are hashed in Insight.

Access permissions are granted on a need to know basis. The headteacher/senior leaders/assessment leads will have full access. Class teachers will have access to their own class' data. No other staff will have access to Insight.

Multi-factor authentication (MFA) is currently being tested by Insight before being rolled out. This will add an extra layer of security once available.

(b) Explain how you will make staff aware of any security measures or procedures they will need to follow

Staff will receive training (internally) on how to use Insight. During this training, security measures and GDPR responsibilities will be made clear and explicit.

Articles 15 – 22: Rights of the data subject

Explain how individual rights (requests for subject access, restriction, rectification, objection, erasure and/or portability) will be managed
All data subject's rights are set out in the school's Privacy Notice for Pupils and Parents.

Articles 44- 49: Transfers of personal data to third countries or international organisations

(a) Explain where the personal data will be hosted, including the routes of transfer if they leave the UK (for example, while most Microsoft cloud services are based in Europe, the data sometimes goes via America)

Insight's primary data is stored with AWS in London, UK, and that other sub-processors are set out in Insights T&Cs - https://www.insighttracking.com/terms#s3 which are all based within the UK (with the exception of transactional emails conducted by Wildbit LLC) and have GDPR compliant contracts in place which include standard contractual clauses.

(b) If the personal data leaves the UK, explain which of the formal / recognised adequacy measures are in place

Standard Contract Clauses (SCCs)

Demonstration of compliancy with data protection legislation (accountability)

(a) Explain what (if any) governance documents will be required to support the data processing (eg Information Sharing Agreements, Data Processor contractual clauses etc)

A Data Processing Agreement (DPA) is in place between the school/TPT and Insight.

(b) Detail what governance arrangements will be in place to oversee the processing of personal data in a compliant manner

Periodic review of this DPIA, and contract/supplier management processes.

4. Consultation

(a) The following consultation approach and stakeholder groups were incorporated into the consultation process:

Headteachers – This document has been reviewed by Warrick Barton at Pensford Primary School.
Assessment Leaders
Central Trust staff

(b) A summary of the stakeholder views:

Following a demonstration of the Insight tracking system, all stakeholders involved could see the educational benefits offered when compared with current system in place (FFT)

(c) The following stakeholder views were taken into consideration and measures to support them have been included in the planned data processing activities:

Financial considerations (comparison of costs between Insight and FFT) have been made. No firm agreement has been made at this stage as we are only involved in a free trial.

(d) The following stakeholder views were considered, but not reflected in the planned data processing activities:

NA

(e) The rationale for not doing so:

NA

Data Protection Impact Assessment

Risk assessment

Privacy issue	*Identify the key privacy risks and associated compliance and corporate risks*			*Describe the actions you could take to reduce the risks*		
	Risk to individual	**Compliance risk**	**Corporate risk**	**Solution(s)**	**Result** *High, medium or low*	**Evaluation** *Is the solution a justified, compliant and proportionate response?*
Insight compromised by hacker	Distress and potential for ID fraud and to be targeted with ransom	GDPR non-compliance which could lead to enforcement action by the regulator (ICO)	Reputational damage	DPO has enquired with Insight on any plans to implement MFA Insight data is encrypted in transit Staff to be trained in cyber security risks – e.g. managing passwords and phishing emails.	M	Y
Access to unauthorised (internal) persons	Low	GDPR non-compliance which could lead to enforcement action by the regulator (ICO)	Reputational damage	School to monitor staff access and swiftly remove users who have moved roles (and no longer need access) or have left	M	Y
Data processed outside of the UK/EEA without sufficient safeguards	Low	GDPR non-compliance which could lead to enforcement action by the regulator (ICO)	Reputational damage	Insight's primary data is held in AWS London, UK. Insight have contracts in place with all sub-processors which include standard contract clauses. School/DPO to monitor Insight ownership/change of control and any changes to their T&Cs or Privacy Notice.	L	Y

Data Protection Impact Assessment

Outcomes

Risk	Approved solution and actions	Approved by	Completion due date	Who is responsible?
Insight compromised by hacker	DPO has enquired with Insight on any plans to implement MFA	TPT/DPO	Multi-factor authentication (MFA) is currently being tested by Insight before being rolled out	DPO and TPT to chase Insight if MFA implementation not done by 1/7/22
	Insight data is encrypted in transit	TPT/DPO	NFA	NFA
	Staff to be trained in cyber security risks – e.g. managing passwords and phishing emails.	TPT/DPO	Training done at some TPT schools, but not all	TPT to consider training options
Access to unauthorised (internal) persons	School to monitor staff access and swiftly remove users who have moved roles (and no longer need access) or have left	TPT/DPO	Ongoing	All school Insight Leads
Data processed outside of the UK/EEA without sufficient safeguards	Insight's primary data is held in AWS London, UK. Insight have contracts in place with all sub-processors which include standard contract clauses.	TPT/DPO	By 30/4/22	TPT to ensure contract/Data Processing Agreement contains SCCs
	School/DPO to monitor Insight ownership/change of control and any changes to their T&Cs or Privacy Notice.	TPT	Ongoing	Schools/TPT to notify DPO of any change in control with Insight
Data subjects not informed of processing	Schools will update Privacy Notices (PNs) to include reference to the use of Insight as a data storage platform and communicate this with parents.	TPT/Schools	By 30/4/22	Each TPT School to add this processing to their PNs

Data Protection Impact Assessment

DPIA authorisation	
Date of consultation with DPO	18/03/2022
Summary of DPO advice	DPO advised on lawful basis and content for Section 3 of the DPIA, along with some risks to consider.
DPO advice accepted or over-ruled by IAO	Accepted by TPT (Sarah Savage 30/3/22)
Rationale for over-ruling the DPO's advice (if applicable)	n/a
Date and name of person referring DPIA to ICO (if applicable)	n/a
Summary of ICO advice	n/a
Date and name of person updating Record of Processing Activity	April 2022 – Warrick Barton