Data Protection Impact Assessment (Insight)

Hurst Green Primary School operates a cloud based system or 'hosted solution', called Insight. Access to Insight is through the internet. Resources are retrieved from Insight via the Internet, through a web-based application, as opposed to a direct connection to a server at the school. Access to Insight is through a web browser. As such Hurst Green Primary School must consider the privacy implications of such a system. The Data Protection Impact Assessment is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action.

Hurst Green Primary School recognises that using a 'hosted solution' has a number of implications. Hurst Green Primary School recognises the need to have a good overview of its data information flow.

The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for a cloud based system and the impact it may have on individual privacy.

The school needs to know where the data is stored, how it can be transferred and what access possibilities the school has to its data. The location of the server is important to determine applicable law. The school will need to satisfy its responsibilities in determining whether the security measures the cloud provider has taken are sufficient, and that the rights of the data subject under the UK GDPR is satisfied by the school.

Hurst Green Primary School aims to undertake a review of this Data Protection Impact Assessment on an annual basis. A Data Protection Impact Assessment will typically consist of the following key steps:

1. Identify the need for a DPIA.
2. Describe the information flow.
3. Identify data protection and related risks.
4. Identify data protection solutions to reduce or eliminate the risks.
5. Sign off the outcomes of the DPIA.

Contents

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

What is the aim of the project? – Hurst Green Primary School The school has identified a need to create a more targeted system which meets the needs of the child, in respect to assessment and reporting, inputting pupil's scores, viewing gap analysis to inform teaching and generating bespoke reports. By using Insight the school will address these issues as follows:

Teachers

- Can record formative and summative assessments from Nursery to Year 6
- Can see everything they need to know about individual pupils on a simple report
- Can see how a class or year group is performing against the school's curriculum targets and spot issues
- Can set targets, record interventions, groups and comments
- A more efficient way for schools to prepare for parents' evening
- Pupil information and statutory assessment data can be directly imported from the schools Management Information System

Senior Leadership Team

- SLT can record teacher assessments, book bands, ages, standardised scores and any other assessments the school is doing
- SLT can generate dynamic reports for all key groups
- Monitor SEN children and vulnerable groups and ensure intervention programmes are having a positive effect
- Quickly see the percentages of cohorts who are on track (including for Reading, Writing and Maths combined)
- Use the Progress Matrix to talk meaningfully about progress, whether or not the school's assessment model gives a 'points' measure

The system will be for internal use only and there will be no sharing of information with outside agencies. Information will be shared only as appropriate with teachers and teaching assistants.

Insight is a hosted system which means that all updates, maintenance and management can be performed in a central location by Insight (Equin Limited is the provider of Insight). The platform is hosted in secure data centres in Eire.

Hurst Green Primary School will undertake the following processes:

1. Collecting personal data
2. Recording and organizing personal data
3. Storing personal data
4. Copying personal data
5. Retrieving personal data
6. Deleting personal data

By opting for Insight the school aims to achieve the following:

1. Management of sensitive pupil information in one place
2. Security and integrity of sensitive data through a secure document vault
3. Storage of information electronically rather than manually
4. Recording information and building a chronology around the pupil
5. Providing bespoke reports for difference audiences, e.g. Parents or agencies
6. Identifying trends and patterns
7. Ability to add information from staff across the school
8. Secure access across all devices wherever the setting

Cloud based systems enable the school to upload documents and other files to a hosted site to share with others within school. These files can then be accessed securely from a PC in the school.

Insight cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated accordingly.

The school is the data controller and Equin Limited is the data processor.

[insert name of school has included Insight within its Information Asset Register.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

The Privacy Notices (pupil) for the school provides the lawful basis of why the school collects data. The lawful basis in order to process personal data in line with the 'lawfulness, fairness and transparency principle is as follows:

6.1 (c) Processing is necessary for compliance with a legal obligation to which the controller is subject; e.g. health & safety and safeguarding

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

6.1 (f) Processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party

The lawful basis for collecting special category information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest and is authorised by domestic law.*

The school has considered the lawful basis by which it processes personal data. This is recorded in Hurst Green Primary School Privacy Notice (Pupil) and where appropriate in Privacy Notice (Workforce).

How will you collect, use, store and delete data? – Insight collects information from pupil records. Personal data relating to the unique pupil number (UPN), pupil legal first and last name, pupil preferred first and last name, date of birth, gender, date pupil joined the school, and date pupil left the school. The personal data is obtained from the schools Management

Information System which may be uploaded via a secure transfer method to the platform's portal.

The information will be stored on the Insight server platform. The information is retained according to the school's Data Retention Policy.

What is the source of the data? – The school's Management Information System.

Will you be sharing data with anyone? – Hurst Green Primary School may share information with teaching professionals including the SENCo, Headteacher, Senior Leadership Team (SLT), Governors, Ofsted and local authority professionals.

What types of processing identified as likely high risk are involved? – The information is transferred securely from the school to the server which is hosted remotely on a server within Eire. Access to information on Insight is controlled through passwords and access controls.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

What is the nature of the data? – Pupil data relates to the unique pupil number (UPN), pupil legal first and last name, pupil preferred first and last name, date of birth, gender, date pupil joined the school, and date pupil left the school.

Insight contains electronic records of the work of the School in identifying assessment needs, monitoring progress and outcomes. These include statutory assessments (e.g. EYFSP,

Phonics, SATs); Test results; Teacher judgements images and written comments supplied as evidence for assessments or as general attachments to pupils' records

Data will be processed in accordance with instructions from Hurst Green Primary School. Insight will not give information to any third parties (other than contractors providing services to Equin Limited with whom an agreement exists) without the consent of Hurst Green Primary School.

Special Category data? – UK GDPR special category data includes race; ethic origin; religion; biometrics; and health.

The following data can optionally be recorded as well: ethnicity, English as an additional language status, free school meal history, SEN history, service child status, In-care status, attendance summaries and customer-defined groups

From the above some of these categories will be special category data is defined under UK GDPR. The lawful basis for collecting special category information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest and is authorised by domestic law.*

How much data is collected and used and how often? – Personal details relating to pupils are obtained from the school's Management Information systems.

In terms of pupil assessment data includes statutory assessments (e.g. EYFSP, Phonics, SATs); Test results; Teacher judgements images and written comments supplied as evidence for assessments or as general attachments to pupils' records.

How long will you keep the data for? – The school follows the good practice in terms of data retention as set out in the IRMS Information Management Toolkit for Schools and also as set out within the school's data retention policy.

Scope of data obtained? – How many individuals are affected (pupils, workforce)? And what is the geographical area covered? EYFS, Year 1 to Year 6 pupils [pupil roll], and workforce [insert number].

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are

there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

What is the nature of your relationship with the individuals? – Hurst Green Primary School collects and processes personal data relating to its pupils to ensure the school provides education to its students with teaching staff delivering the National Curriculum.

Through the Privacy Notice (Pupil) Hurst Green Primary School is committed to being transparent about how it collects and uses data and to meeting its data protection obligation.

How much control will they have? – Access to the data held on Insight will be controlled by username and password. The platform will be used internally only from devices based within the school. Access to the platform can be revoked at any time.

Do they include children or other vulnerable groups? – All of the data will relate to children.

Are there prior concerns over this type of processing or security flaws? – How is the information stored? Does the cloud provider store the information in an encrypted format? What is the method of file transfer? How secure is the network and what security measures are in place?

Hurst Green Primary School recognises that moving from a manual system to an electronic system which holds sensitive personal data in the cloud raises a number of General Data Protection Regulations issues as follows:

- **ISSUE:** Insight will be storing personal data.
  RISK: There is a risk of unauthorized access to information by third parties.
  MITIGATING ACTION: Personal data is hosted on Amazon Web Services (AWS)

  Amazon take physical and network security seriously. Their data centres are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at

building ingress points by professional security staff, video surveillance, intrusion detection systems, and other electronic means

Access to their data centre floors requires two-factor authentication a minimum of two times. Insight system access to the database is via a secure, password-protected, connection

As described in Insight's Terms of Service, schools must provide each of their Authorised Users with their own access to Insight via an email address and password. Commonly used passwords which are known to have been previously leaked will be refused, to help ensure that secure passwords are chosen

Passwords are stored in a hashed form. Insight cannot view school passwords – if the school needs to reset it, it will need to follow the password reset procedure

- **ISSUE**: Transfer of data between the school and the cloud.
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: Insight is a web-based application, accessible only over a secure (https) connection. This ensures all data is encrypted while in transit

  All access to the data via web browser is encrypted. Insight are in the process of migrating to a new database that will support encryption of data at rest. This should be completed by the end of the year

- **ISSUE:** Use of third party sub processors?
  RISK: Non compliance with the requirements under UK GDPR
  MITIGATING ACTION: Equin Limited use carefully selected processors and sub-processors to deliver Insight and to operate the business. These third parties supply the infrastructure, storage and associated services necessary for Equin Limited to provide Insight. Equin Limited have entered into UK GDPR-compliant, written contracts with its processors and sub-processors
  Where Equin Limited see a need to add a new sub-processor to those specified, Equin Limited will first notify the school to explain their purposes, and the school will have the opportunity to object

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: Insight's primary infrastructure and the school's data is hosted on Amazon Web Services, Inc. ("AWS"), which is a global leader in Infrastructure as a Service ("IaaS"). Equin Limited use AWS's data centre in Ireland, ensuring that sensitive data remains stored within the EU

  All of Insight's data is stored in a single database . A school ID is used to determine which data records belong to which school. All access via the Insight web application include a school ID, which is used to filter results to the right school.

- **ISSUE:** Cloud solution and the geographical location of where the data is stored
  RISK: Within the EU, the physical location of the cloud is a decisive factor to determine which privacy rules apply. However, in other areas other regulations may apply which may not be Data Protection Law compliant
  MITIGATING ACTION: Data centres are based in Eire. This means that the UK GDPR privacy rules apply to the cloud based service

- **ISSUE:** The right to be informed; the right of access; the right of rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object
  RISK: The school is unable to exercise the rights of the individual
  MITIGATING ACTION: User permissions within Insight ensure that schools are able to fully comply with their obligations with regard to the exercise of data subjects' rights

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Equin Limited retain personal information for up to 12 months following any contact, or for as long as the school is a customer of or has a free trial of Insight, or indefinitely as required to keep track of requests not to be contacted

  The school may at any time delete or export, or ask Equin Limited to delete or export, any customer data that is no longer required to process. Otherwise, customer data is

retained until the agreement with Equin Limited terminates, and will be deleted within 30 days of that termination

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Any data breaches are recorded in the Insight internal log. Equin Limited would notify the school via the account's primary email address, within 72 hours of detecting a breach. If Equin Limited think the breach is very serious then the company would attempt to contact the school via telephone as well

  The school will recognize the need to define in their contract a breach event and procedures for notifying the school and the school managing it

- **ISSUE:** Data is not backed up
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Insight's primary server is replicated to a secondary database and is backed up daily at midnight to prevent data loss. The Software database is also replicated in real time to a secondary database

  Backups are securely stored in a separate location and are also password-protected

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Data is stored in Eire within secure Data Centres, with backups as standard. Post Brexit the UK is outside of the European Economic Area ("EEA")

  The UK has an approved Adequacy Agreement with the EU and therefore post Brexit GovernorHub will continue to remain compliant with the provision of cloud storage held within the EU. This means that the school remains GDPR compliant when using GovernorHub

  With regards to Insight use of servers in Eire, the UK will recognise all EEA states, EU and EEA institutions, and Gibraltar as providing an adequate level of protection for personal data. This means that personal data can continue to flow freely from the UK to these destinations following the UK's exit from the EU

As a further contingency, Insight have the option to move database servers and web servers to a UK based data centre. Equin Limited might require Insight to be offline for a day while the migration happens

- **ISSUE:** Subject Access Requests
  RISK: The school must be able to retrieve the data in a structured format to provide the information to the data subject
  MITIGATING ACTION: User permissions within Insight ensure that schools are able to fully comply with their obligations with regard to the exercise of data subjects' rights

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: As Data Controller the school maintains ownership of the data. Equin Limited is the data processor

- **ISSUE:** Cloud Architecture
  RISK: The school needs to familiarise itself with the underlying technologies the cloud provider uses and the implications these technologies have on security safeguards and protection of the personal data stored in the cloud
  MITIGATING ACTION: Insight's primary server is replicated to a secondary database and is backed up daily to prevent data loss

- **ISSUE:** UK GDPR Training
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to Insight
- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Equin Limited takes security seriously and has processes to protect customer information.

  Equin Limited is registered with the ICO (registration number is Z1904040)

  Amazon Web Services (AWS) 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 more can be read about the specifics of their approach at https://aws.amazon.com/security/

ISO 27001: is one of the most widely recognized, internationally accepted independent security standards. Google has earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centers that make up its shared Common Infrastructure as well as for GSuite and Google Cloud Platform

For further information please read the Privacy Notice (Insight)

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The school moving to a cloud based solution will realise the following benefits:

1. Management of sensitive pupil information in one place
2. Security and integrity of sensitive data through a secure document vault
3. Storage of information electronically rather than manually
4. Recording information and building a chronology around the pupil
5. Providing bespoke reports for difference audiences, e.g. Parents or agencies
6. Identifying trends and patterns
7. Ability to add information from staff across the school
8. Secure access across all devices wherever the setting

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

The views of senior leadership team will be obtained. Once reviewed the views of stakeholders will be taken into account

The view of YourIG has also been engaged to ensure Data Protection Law compliance

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The lawful basis for processing personal data is contained in the school's Privacy Notice (Pupil). The lawful basis includes the following:

- Health and Safety at Work Act
- Keeping Children Safe in Education
- Safeguarding Vulnerable Groups Act
- Working together to Safeguard Children Guidelines (DfE)

The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law. Insight will enable the school to uphold the rights of the data subject; the right to be informed; the right of access; the right of rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object; and the right not to be subject to automated decision-making; these rights will be exercised according to safeguarding considerations.

The school will continue to be compliant with its Data Protection Policy.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Data transfer; data could be compromised	Possible	Severe	Medium
Asset protection and resilience	Possible	Significant	Medium
Data Breaches	Possible	Significant	Medium
Post Brexit (GDPR noncompliance)	Possible	Significant	Medium
Subject Access Request	Probable	Significant	Medium
Upholding rights of data subject	Probable	Significant	Medium
Data Retention			

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no
Data Transfer	Secure network, end to end encryption	Reduced	Medium	Yes
Asset protection & resilience	Data Centre based in Eire	Reduced	Medium	Yes
Data Breaches	Documented in contract and owned by school	Reduced	Low	Yes
Post Brexit	Contingency plans insitu from the supplier	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes
Upholding rights of data subject	Technical capability to satisfy rights of data subject	Reduced	Low	Yes
Data Retention	Implementing school data retention periods as outlined in the IRMS Information Management Toolkit for Schools	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Headteacher	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Headteacher	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Yes	DPO should advise on compliance, step 6 measures and whether processing can proceed

Summary of DPO advice: Technical recommendations to be clarified with third party as follows:

(1) How is the information stored on the server? (e.g. is the server shared with other schools, what security is in place to maintain the integrity of the school's data?)

All of Insight's data is stored in a single database. A school ID is used to determine which data records belong to which school. All access via the Insight web application include a school ID, which is used to filter results to the right school.

(2) Do you store the information in an encrypted format? (if not how is the information stored?)

The database is not currently encrypted at rest. All access to the data via web browser is encrypted. We are in the process of migrating to a new database that will support encryption of data at rest. This should be completed by the end of the year.

(3) Data is stored in Eire within secure Data Centres, with backups as standard. What are the third party contingency arrangements in the event of a no deal Brexit.

We have the option to move database servers and web servers to a UK based data centre. We might require Insight to be offline for a day while the migration happens.

(4) How would the supplier respond to a data breach and how would the school be notified?

Any data breaches are recorded in our internal log. We would notify your school via the account's primary email address, within 72 hours of detecting a breach. If we think the breach is very serious then we'd attempt to contact the school via phone as well.

DPO advice accepted or overruled by: No If overruled, you must explain your reasons
Comments:
Consultation responses reviewed by: Headteacher If your decision departs from individuals' views, you must explain your reasons
Comments:
This DPIA will kept under review by: School Business Manager The DPO should also review ongoing compliance with DPIA