Data Protection Impact Assessment (Little Wandle Letters and Sounds)

Hurst Green Primary School operates a cloud based system or 'hosted solution', called Renaissance Learning. Access to Little Wandle is through the internet. Information is retrieved from Renaissance Learning via the Internet, through a web-based application, as opposed to a direct connection to a server at the school. 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? – Little Wandle is a complete phonics programme designed to improve the teaching of reading in Reception and Key Stage 1 (early primary phase) and ensure all children become fluent readers.

The programme is validated by the Department for Education (DfE).

In order to deliver this programme, Wandle Learning Trust collects data on teachers and other staff in schools, as well as on the pupils they teach. The data processing involves analysis of teachers' own self-assessment (CPD) and their assessments of their pupils, as well as administration of website access, communication and invoicing.

The DPIA has been put in place due to the likely high-risk processing below and to be able to evaluate the risk and reduce any risks to an acceptable level.

- Evaluation or scoring
- Data processed on a large scale
- Matching or combining datasets
- Data concerning vulnerable data subjects.

The DPIA has also been developed to allow a full overview, allowing a greater understanding of how all parties data is used and any associated risks involved.

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 Little Wandle 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 different 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

Where the school had a previous electronic system t was recognized that this system had limitations and with the school investing in the Little Wandle suite of applications, additional benefits can be realized.

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.

Wandle Learning Trust 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 Renaissance Learning is the data processor.

Hurst Green Primary School has included Little Wandle 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? – Little Wandle collects information from pupil records, Special Educational Needs (SEN) records and behavior records. Information System. The information will be stored in Renaissance Learning. The information is retained according to the school's Data Retention Policy.

Data is collected from teachers and other staff entering data onto the Letters & Sounds website. This is a combination of direct, manual data entry into the main Letters & Sounds

Wordpress website or embedded Google Forms, and the upload of pupil data in a CSV file directly into the analysis website (https://analysis.littlewandlelettersandsounds.org.uk).

What is the source of the data? – Pupil information is collected via registration forms when pupils join the school, pupil update forms the school issue at the start of the year, Common Transfer File (CTF) or secure file transfer from previous schools. Pupil information also includes classroom work, assessments and reports. SENCO records, Education Health and Care Plans, Pupil Records, and Early Help Assessment.

Little Wandle collects personal data through a combination of direct, manual data entry into the main Letters & Sounds Wordpress website or embedded Google Forms, and the upload of pupil data in a CSV file directly into the analysis website (https://analysis.littlewandlelettersandsounds.org.uk).

Will you be sharing data with anyone? – Hurst Green Primary School may share information with education professionals including the SENCo, Headteacher, Senior Leadership Team (SLT), Governors, Ofsted, the local authority. However, this does not mean that Hurst Green Primary School shares Little Wandle access to the third parties.

What types of processing identified as likely high risk are involved? – Transferring 'special category' data from the school to the cloud. Storage of personal and 'special category data in the Cloud.

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? – The personal data on staff includes name, school, role and contact details.

The personal data on children includes name, unique pupil number and demographic characteristics (date of birth, ethnicity, gender, year group, special educational need

provision, first language, free school meal status), so is sensitive data including protected characteristics.

Assessment data is also collected for both staff and pupils. Staff complete one-off training and answer a series of multiple-choice questions to check their understanding and recall.

Separately, teachers run assessments with pupils and record whether each pupil correctly sounded an individual word or grapheme (the letter or letters that represent a sound in writing). This happens across six assessment points each year. Some financial information is held in PS Financials, in particular the school subscription cost (which is related to the size of school).

Staff data is used to administer access to the website and communicate with staff involved in Letters & Sounds, as well as ensure that staff have a good understanding of the phonics teaching. Pupil data is used to help assess children and analyse progress and gaps in understanding for individuals and groups of pupils.

Special Category data? – Data revealing ethnic origin, special education need provision are collected by the school and contained in Little Wandle. 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 parent/pupil information systems. Additional content is obtained from classroom/teacher observation/agency partners. This also includes recorded information and reports.

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 the schools data retention policy.

Scope of data obtained? – How many individuals are affected (180 for safeguarding issues and concerns) and for pastoral issues (approximately 180 pupils). The geographical area covered is from pupils in Reception to Key Stage 1.

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. It also collects and processes personal data relating to its pupils to manage the parent/pupil relationship. Personal data is collected for the workforce to assist with the creation of login accounts dependent on job role.

Through the Privacy Notice (Pupil) and (Workforce) 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? – Not all staff will have access to Renaissance Learning. The school can restrict access to Renaissance Learning so that only designated staff only see information that is relevant to them. Access to the data held on Renaissance Learning will be controlled by username and password.

Additionally, whilst Renaissance Learning works on any device with access to the internet, staff that are granted access to the system will have to utilise an additional password of their own, which is only shared between authorized members of staff at the school. School administrators have full access to the system, which are defined by permissions.

Do they include children or other vulnerable groups? – All of the data will relate to children. The information will relate to learning assessment, etc.

Are there prior concerns over this type of processing or security flaws? – All data is secured in transit using modern TLS standards used throughout the industry.

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

- **ISSUE:** Little Wandle will be storing personal data
  RISK: There is a risk of unauthorized access to information by third parties
  MITIGATING ACTION: The staff details data is stored on a Wordpress server and also transferred to Hubspot servers for communication purposes. This may mean some teacher data is stored outside of the EU.

  A Standard Contractual Clauses (SCC) is in place for these third parties. Teacher assessments are stored in Google Sheets held in an EU G Suite account. Pupil assessments are stored in Google Sheets then transferred to a UK database server. Pupil details are uploaded directly into a UK server. Letters & Sounds data stored within the Trust is stored on OneDrive within the EU, with all Letters & Sounds IT access following standard IT practices including encryption for all mobile devices. Normally no paper copies of data will be stored although schools may choose to print out assessment data for their own records.

  Penetration testing is undertaken an annual basis. Security patches are installed. Little Wandle use Microsoft 365 activity logging, and data base logs for cloud servers (i.e. AWS).

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred
  MITIGATING ACTION: All connections to the Assessment Tracker website are encrypted over SSL. The https:// (instead of the normal http://) in the school's browser's address bar denotes an SSL connection, which means any data transferred is encrypted before being sent.

  All files are encrypted at Bitlocker Encryption (256-bit) which is the highest level available. SSL encryption takes place between the school's computer and the Little Wandle server.

  Mime machines are protected with Bitlocker Encryption (256-bit). The Assessment Tracker is hosted with AWS and encrypted at rest (Amazon EBS encryption).

- **ISSUE:** Use of third party sub processors?
  RISK: Non-compliance with the requirements under UK GDPR
  MITIGATING ACTION: Mime, an education data consultancy, is a data sub-processor for the pupil data and teacher assessment data. Communitas, a specialist education communications agency, is a data sub-processor for staff data. All sub-processors have a compliant privacy notice clearly displayed.

  Data is only shared with staff involved in Letters & Sounds and within a school (i.e. it will never be shared between schools). Data will never be shared with any third parties apart from data sub-processors named in the Letters & Sounds privacy policy or other staff and associates working on the Letters & Sounds programme.

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: Best practice security measures are used to protect personal data, including security certificates on websites, use of encrypted laptops for any data held locally, and strong password standards.

  All staff at Mime involved in the processing of pupil data are DBS checked and sign an information security policy. They also do data protection training as part of their induction and refreshers as policies are updated.

- **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: All data will be held within the EU.

If data was stored outside of the EU a Standard Contractual Clauses (SCC) would be in place for these third parties. Teacher assessments are stored in Google Sheets held in an EU G Suite account.

Pupil assessments are stored in Google Sheets then transferred to a UK database server. Pupil details are uploaded directly into a UK server.

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Access to data is limited to staff approved by each school. Much of this access is limited to the headteacher, a named 'Reading Leader' or another named 'Super User' (for example, at present only the Super User will be able to access pupil assessment analysis).

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Data will normally be retained for as long as a school is a licence holder then an additional 2 years after the end of the licence period, or when a school requests that their account and all associated pupil data is deleted. Teacher and pupil data can also be manually deleted by schools.

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Little Wandle has policies and procedures in place to ensure schools are notified in the event of data breaches as required by UK GDPR.

  If the school becomes aware of a breach it will contact the Data Protection Officer for Little Wandle.

- **ISSUE:** Data is not backed up
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Backups are taken continuously throughout the day, dependent on the data store this will determine which schedule the backup falls into. The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after

an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

All backups are encrypted before being stored using keys from Amazon Key Management. The keys are rotated yearly and all keys required to decrypt existing backups will be stored until no longer required.

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: All data will be held within the EU. If data was stored outside of the EU a Standard Contractual Clauses (SCC) would be in place for these third parties. Teacher assessments are stored in Google Sheets held in an EU G Suite account.

  Pupil assessments are stored in Google Sheets then transferred to a UK database server. Pupil details are uploaded directly into a UK server.

- **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: Little Wandle has the capability to provide the schools with access to the data stored within. Where Subject Access Requests are made for specific areas of school data Little Wandle can either provide, or will provide, means for authorised client users to carry out activities directly. Little Wandle will direct enquiries where parents have identified erroneous information, back to the school.

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: As Data Controller the school maintains ownership of the data. Little Wandle 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: All data will be held within the EU. If data was stored outside of the EU a Standard Contractual Clauses (SCC) would be in place for these third parties. Teacher assessments are stored in Google Sheets held in an EU G Suite account.

Pupil assessments are stored in Google Sheets then transferred to a UK database server. Pupil details are uploaded directly into a UK server.

Where security updates are applicable to the infrastructure, Amazon Web Services will manage these.

- **ISSUE:** UK GDPR Training
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to Little Wandle.

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The data gathered about students via the Little Wandle Letter and Sounds website will be shared with Mime Consulting Ltd ("Mime"), but remains the responsibility of Wandle Learning Trust.

  ICO Registration: Mime and Little Wandle are registered with the Information Commissioner's Office (ICO) for data protection, the UK's independent supervisory authority, that upholds public information rights and regulatory controls in the use of personal data by data controllers such as schools.

  Mime's registration with the Information Commissioners Office is (reference Z1059351).

  Little Wandle's registration with the Information Commissioners Officer is (reference ZA517258).

  ISO 27001: The Assessment Tracker is hosted by Amazon Web Services (AWS). AWS have ISO 27001: is one of the most widely recognized, internationally accepted independent security standards. AWS has earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centres that make up its shared Common Infrastructure.

  The following hyperlink details security procedures - https://aws.amazon.com/security/

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

Renaissance Learning 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
Subject Access Request	Probable	Significant	Medium
Upholding rights of data subject	Probable	Significant	Medium
Data Retention	Probable	Significant	Medium

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	Depending on the product selected data centres located in the UK or elsewhere Standard Contractual Clauses in place	Reduced	Medium	Yes
Data Breaches	Documented in contract and owned by school	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 and data retention policy	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) Transfer of data between the school and the cloud, i.e. AES 256-bit encryption . Is the data encrypted end to end and whilst at rest. (2) How often is data back up? (3) Does Little Wandle have industry recognized accreditation, i.e. ISO 27001 The responses have been embedded in the Issue, Risk and Mitigation Action log as documented in Step 2 of this DPIA		
DPO advice accepted or overruled by: Accepted If overruled, you must explain your reasons		
Comments:		
Consultation responses reviewed by: DPO 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