STUART BATHURST CATHOLIC HIGH SCHOOL

Data Protection Impact Assessment

(Renaissance Learning)

Data Protection Impact Assessment (Renaissance Learning)

Stuart Bathurst Catholic High School operates a cloud-based system or 'hosted solution', called Renaissance Learning. Access to Renaissance Learning 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. Access to Renaissance Learning is through a web browser. As such Stuart Bathurst Catholic High 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. Stuart Bathurst Catholic High School recognises that using a 'hosted solution' has a number of implications. Stuart Bathurst Catholic High 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.

Stuart Bathurst Catholic High School aims to undertake a review of this Data Protection Impact Assessment on an annual basis.

What is the aim of the project?

Stuart Bathurst Catholic High School will use the system as an online platform for assessing pupils reading and mathematics ability, to help develop the pupil's learning and skills development.

All teaching staff will have access to the system, including a limited number of support staff. Access is dependent on job role and need. Renaissance Learning provides a level of access to facilitate this requirement.

Renaissance Learning is a hosted system which means that all updates, maintenance and management can be performed in a central location by Renaissance Learning UK Limited.

Renaissance Learning is an instant assessment and tracking system which comprises of a suite of products, depending on the school's need. Star Assessments complement the student applications Accelerated Reader, Accelerated Maths and myON which provide a personalised learning plan for each student, helping to inform next steps. Testing can be tailored to the individual pupil's need. Stuart Bathurst Catholic High School hopes to achieve ease of management of the assessment of reading and numeracy abilities by adopting the platform.

The platform provides a number of tools with which to help develop students learning and also reporting tools for teachers.

Stuart Bathurst Catholic High School will undertake the following processes:

- Collecting personal data
- Recording and organizing personal data
- Storing personal data
- Copying personal data
- Retrieving personal data
- Deleting personal data

By opting for Renaissance Learning the school aims to achieve the following:

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

Where the school had a previous electronic system Stuart Bathurst Catholic High School it was recognized that this system had limitations and with the school investing in the Renaissance Learning 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.

Renaissance Learning 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.

Stuart Bathurst Catholic High School has included Renaissance Learning within its Information Asset Register.

The Privacy Notices (pupil) for the school provides the legitimate basis of why the school collects pupil data. Specifically, this relates to health and safety and safeguarding of vulnerable groups. Renaissance Learning is referenced in the respective Privacy Notices.

How will you collect, use, store and delete data?

Renaissance Learning collects information from pupil records, Special Educational Needs (SEN) records and behavior records. The school has a choice how it populates the Renaissance Learning system, either through a webform, manually via a CSV file, or a data sharing agreement is in place with Wonde if the school chooses an automated approach, linking to Stuart Bathurst Catholic High School Management Information System. The information will be stored in Renaissance Learning. The information is retained according to the school's Data Retention Policy.

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.

Renaissance Learning collects personal data from the school's management information system.

Will you be sharing data with anyone?

Stuart Bathurst Catholic High 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 Stuart Bathurst Catholic High School shares Renaissance Learning 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.

What is the nature of the data?

Pupil data relates to personal identifiers and contacts (such as name, tutor, teaching group membership). Information that is processed (but not limited to): pupils' names, pupils' data (including SEN status, Pupil Premium status, gender and class year groups; This data is optional and does not need to be entered into the platform.

Workforce data relates to personal information (such as name, email address, phone number, tutor group(s) and teaching groups. Only enough information is collected for the school to create a login account for the member of staff and assign the student groups they are assigned to.

Special Category data?

Data revealing racial or ethnic origin, medical details are collected by the school and contained in Renaissance Learning. The lawful basis for collecting this information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.*

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.

SEND information is transferred to the receiving school as part of the pupil record. This is signed for by the receiving school. This is then kept by the receiving school from DOB of the child + 31 years then reviewed.

Scope of data obtained?

Data will relate to students at Stuart Bathurst Catholic High School

What is the nature of your relationship with the individuals?

Stuart Bathurst Catholic High 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) Stuart Bathurst Catholic High 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.

Stuart Bathurst Catholic High 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: Renaissance Learning will be storing personal data
RISK: There is a risk of unauthorized access to information by third parties
MITIGATING ACTION: Renaissance Learning UK Ltd school data is stored on approved and compliant cloud infrastructure. Access to all parts of the infrastructure is available to Renaissance Learning UK Ltd staff on a need to know basis and access is always revoked as soon as a member of staff no longer needs access or leaves the company. User access is based on individual usernames and passwords

Security related updates for all software used across the infrastructure is installed in a timely manner

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 a Renaissance Learning installation 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

The SSL certificate also allows the school's computer to verify that the Renaissance Learning server is the server it says it is. Connections are encrypted with 256-bit AES encryption with 2048-bit keys. AES encryption is a US government standard for encryption, and 256-bit is the highest level available. SSL encryption takes place between the school's computer and the Renaissance Learning server when accessing Renaissance Learning and between the school's MIS and the Renaissance Learning server when school data is being transferred through an automatic extract

In addition to the SSL encryption, which ensures data transfer between the school's computer and the Renaissance Learning server, and the school's MIS and the Renaissance Learning server, is encrypted, Renaissance Learning also perform data encryption on any sensitive information stored in the Renaissance Learning databases

All staff employed by Renaissance Learning Ltd who work on Renaissance Learning (including agents and subcontractors) shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty or otherwise), and shall not permit any person to process the data who is not under such

a duty of confidentiality. Authorised persons shall only access the data only as necessary for the permitted purpose

ISSUE: Understanding the cloud-based solution chosen where data processing/storage premises are shared?
RISK: The potential of information leakage
MITIGATING ACTION: Renaissance Learning UK Ltd's servers are hosted according to the product that has been purchased by Stuart Bathurst Catholic High School

The myON product is hosted by Amazon Web Services located in the UK region

Accelerated Reader and Star products are hosted at the data centre located in Wisconsin, United States. Backups for Accelerated Reader and Star are hosted in Amazon Web Services (US region)

Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements

Physical access is controlled at building ingress points by professional security staff utilising surveillance, detection systems, and other electronic means. Authorised staff utilise multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open

Amazon Web Services (AWS) provides physical data centre access only to approved employees. All employees who need data centre access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requestors must specify to which layer of the data centre the individual needs access to and are time-bound. Requests are reviewed and approved by authorised personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions

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: Renaissance Learning UK Ltd customer data is hosted according to the product employed by the school. Renaissance participates in and complies with the EU-US Privacy Shield Framework as set forth by the United States Department of Commerce regarding the collection, use and retention of Personal Data transferred from the European Union and the United Kingdom to the United States in reliance on the Privacy Shield

The European Court of Justice (ECJ) has ruled that the EU-US Privacy Shield is invalid as it fails to protect privacy and data protection rules. As part of the same ruling the ECJ decided that another data transfer mechanism, Standards Contractual Clauses, or SCCs, remain valid. The school will need to confirm whether an SCC is in place

ISSUE: Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
RISK: UK GDPR non-compliance
MITIGATING ACTION: Where it is necessary to access school data only approved Renaissance Learning UK Ltd staff can access it. All employees complete annual Global Privacy and Information Security training. Additionally, all employees sign confidentiality agreements

ISSUE: Implementing data retention effectively in the cloud
RISK: UK GDPR non-compliance
MITIGATING ACTION: Renaissance Learning UK Ltd follows the school's data retention policy; where information is updated in the schools MIS system, this is reflected in the Renaissance Learning UK Ltd servers. Where the school terminates its subscription to the Services with Renaissance Learning, a 60-day grace period is given before personal data is removed from the Services. Following the 60-day grace period, personal data is removed from primary storage facilities within 30 days and from all backups after 90 days

ISSUE: Responding to a data breach
RISK: UK GDPR non-compliance
MITIGATING ACTION: Renaissance Learning 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 Renaissance Learning UK Ltd contact concerning security issues, serious or minor. In the event of a serious incident, the school will have the full support of the company's technical team as a matter of priority until the issue is resolved

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.

ISSUE: Post Brexit
RISK: UK GDPR non-compliance
MITIGATING ACTION: Renaissance Learning have identified mechanisms in order to provide continuity of service Post Brexit

Where data originates from the European Union and is received by the UK (eg. myON UK AWS server, customer support, sales, similar functions), Renaissance Learning state that until the EU makes an adequacy decision with respect to the UK, transfers shall be made in accordance with UK GDPR Article 49(1)(c), Derogations for Specific Situations or, if requested by a school, under model clauses

Where the data originates from the European Union and is received by the United States (e.g. Renaissance products; support functions for myON UK), there will be no impact - EU-US Privacy Shield still applies to EU to US personal data transfers

Where the data originates from the UK and the European Union is the recipient country, there is no change

Where the data originates from the United Kingdom and the recipient is the United States, then the EU-US Privacy Shield applies, with slight modifications at the end of the transition period on the 31st of December 2020. These can be found at:- https://www.privacyshield.gov/article?id=Privacy-Shield-and-the-UK-FAQs

The European Court of Justice (ECJ) has ruled that the EU-US Privacy Shield is invalid as it fails to protect privacy and data protection rules. As part of the same ruling the ECJ decided that another data transfer mechanism, Standards Contractual Clauses, or SCCs, remain valid. The school will need to confirm whether an SCC is in place

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: Renaissance Learning 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 Renaissance Learning UK Ltd can either provide, or will provide, means for authorised client users to carry out activities directly. Renaissance learning 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. Renaissance Learning 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: Renaissance Learning UK Ltd through the employment of Amazon Web Services are using the global Security Operations Centres, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses. This should be monitored to address any changes in technology and its impact on data. The school should maintain ownership of the Cloud technologies used ensuring the current and future technologies enable UK GDPR compliance

Renaissance Learning can also automatically scale to meet increased platform demand, by adding or removing capacity as required

ISSUE: UK GDPR Training
RISK: UK GDPR non-compliance
MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to Renaissance Learning. All employees complete annual Global Privacy and Information Security training

ISSUE: Security of Privacy
RISK: UK GDPR non-compliance
MITIGATING ACTION: Amazon Web Services hold compliance with ISO/IEC 271001:2013, 27017:2015 and 27018:2019. Renaissance Learning UK Ltd ICO registration number Z8942562

ISO 27001: is one of the most widely recognized, internationally accepted independent security standards. Renaissance Learning has earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centres that make up its shared Common Infrastructure

ISO 27017: is an international standard of practice for information security controls based on ISO/IEC 27002, specifically for Cloud Services. Renaissance Learning has been certified compliant with ISO 27017 for its shared Common Infrastructure

ISO 27018: is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services. Renaissance Learning has been certified compliant with ISO 27018 for its shared Common Infrastructure

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

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

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

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.

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

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 in the US with need for a Standard Contractual Clause	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

Item	Name/date	Notes
Measures approved by:	Richard May	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Richard May	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	No	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:		
DPO advice accepted or overruled by: If overruled, you must explain your reasons		
Comments:		
Consultation responses reviewed by: If your decision departs from individuals' views, you must explain your reasons		
Comments:		
This DPIA will kept under review by:	Alicia Mortimer	The DPO should also review ongoing compliance with DPIA