STUART BATHURST CATHOLIC HIGH SCHOOL

Data Protection Impact Assessment (Core5)

Data Protection Impact Assessment (Core5)

Stuart Bathurst Catholic High School operates a cloud-based system or 'hosted solution', called LexiaUK Core5. Access to Core5 is through the internet. Information is retrieved from Core5 via the Internet, through a web-based application, as opposed to a direct connection to a server at the school. Access to Core5 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 considering 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 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?

A specific number of teaching staff have been identified as requiring access to the system. Access is dependent on job role and need. LexiaUK's Core5 product provides a level of access to facilitate this requirement.

Core5 is a hosted system which means that all updates, maintenance and management can be performed in a central location by LexiaUK Limited.

Core5 Reading provides all students, from at-risk to on-level and advanced, a systematic and structured approach to the six areas of reading, covering early phonological to advanced comprehension skills. The program creates personalised learnings paths for each student through an adaptive placement and scaffolded activities. Stuart Bathurst Catholic High School hopes to achieve ease of management of the assessment of reading by adopting the platform. The platform provides a number of tools with which to help develop students learning and also reporting tools for teachers.

By employing Core5, the school aims to realise benefits by adopting a common platform to improve processes, secure remote access and identifying issues which can then be shared across all those staff that have access through centrally-managed training.

Stuart Bathurst Catholic High 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 Core5 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

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.

LexiaUK 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 LexiaUK is the data processor.

Stuart Bathurst Catholic High School has included Lexia Core5 within its Information Asset Register.

Note that where 'LexiaUK' is mentioned in this DPIA, this also includes the parent company LexiaUS which hosts and performs some of the data processing functions on behalf of the school.

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. Core5 is referenced in the respective Privacy Notices.

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

Core5 collects information from pupil records, Special Educational Needs (SEN) records and behavior records. Student details are added individually through the secure portal. Staff records are added individually through the secure portal. The information will be stored in Core5. 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.

Workforce information is collected through application forms, CVs or resumes; information obtained from identity documents, forms completed at the start of employment, correspondence, interviews, meetings and assessments.

Stuart Bathurst Catholic High School recognize the importance of GDPR principle of Article 5 1 (c) "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (the principle of data minimisation).

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 Core5 access to the third parties.

In terms of sharing data with Core5 Stuart Bathurst Catholic High School will apply the GDPR principle of Article 5 1 (c) “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed” (the principle of data minimisation).

The lawful basis for Stuart Bathurst Catholic High School in collecting this information relates to Article 9 2 (b) *processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in respect to* The Children Act and subsequent amendments and The Education Act. The lawful basis is also covered by Schedule 1, part 2, paragraph 8 (Substantial Public Interest Conditions - equality of opportunity or treatment). This is further documented in the school’s Privacy Notice.

The WAN link from the school is a dedicated lease line so is not shared with other users like domestic broadband users, therefore it is protected from interception.

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, instructional language, ethnicity and class year groups); This data is optional and does not need to be entered into the Tracker in that is can be anonymised.

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 Core5.

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.

In terms of sharing data with Core5 Stuart Bathurst Catholic High School will apply the GDPR principle of Article 5 1 (c) “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed” (the principle of data minimisation).

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.

What is the nature of your relationship with the individuals?

Stuart Bathurst Catholic High School collects and processes personal data relating to its pupils and employees to manage the parent/pupil and employment relationship.

Through the Privacy Notice (pupil/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 Core5. The school can restrict access to Core5 so that only designated staff only see information that is relevant to them. Access to the data held on Core5 will be controlled by username and password.

Additionally, whilst Core5 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?

LexiaUK employs cloud hosting services which has ISO 27001 accreditation, which is the international standard for information security management.

Stuart Bathurst Catholic High School] recognises a number of UK General Data Protection Regulations issues as follows:

- **ISSUE:** LexiaUK will be storing personal data.
  RISK: There is a risk of unauthorized access to information by third parties.
  MITIGATING ACTION: LexiaUK school data is stored on approved and compliant cloud infrastructure. Access to all parts of the infrastructure is available to LexiaUK staff on a permissions-level basis so that only those members of staff that require access, are granted the appropriate permissions. In addition, LexiaUK have appropriate policies, procedures, physical and technical controls in place which are designed to manage access to appropriate persons.

- **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 Core5 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 Core5 server is the server it says it is. Connections are encrypted with 256-bit AES encryption. AES encryption is a US government standard for encryption, and 256-bit is the highest level available.

- **ISSUE:** Understanding the cloud-based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage.
  MITIGATING ACTION: LexiaUK's servers are hosted by Amazon Web Services located in the United States.

  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: LexiaUK's servers are hosted by Amazon Web Services in the United States. LexiaUK provides a Standard Contract Clause statement at:-

  https://www.lexialearning.com/I-DPA

  Which clarifies the equivalent standards to the UK GDPR that LexiaUK will adhere to, in respect to International Data Transfers.

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: GDPR non-compliance
  MITIGATING ACTION: Where it is necessary to access school data only approved LexiaUK staff can access it. LexiaUK have appropriate policies, procedures, physical and technical controls in place which are designed to manage access to appropriate persons. LexiaUK provide regular training on their information security and data policies and procedures to their personnel who are responsible for or have access to Student Records.

- **ISSUE:** Implementing data retention effectively in the cloud.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: LexiaUK follows the school's data retention policy; data is managed and updated by the school. Upon the termination of the data processing contract at the choice of the school, LexiaUK will return all the personal data transferred to the school or LexiaUK shall destroy all the personal data and certify to the school that it has done so, unless legislation imposed upon LexiaUK prevents it from returning or destroying all or part of the personal data transferred.

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

  If the school becomes aware of a breach it will contact the named LexiaUK 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: 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:** No deal Brexit.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: Core5 servers are hosted in the US. LexiaUK stipulates in its Standard Contract Clause that equivalent to, or greater than the standards expected than the UK GDPR will be adhered to for cross-border transfers (part 5 and Annex A as identified in the following statement at: https://www.lexialearning.com/I-DPA).

- **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: LexiaUK 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 LexiaUK can either provide, or will provide, means for authorised client users to carry out activities directly.

- **ISSUE:** Data Ownership.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: As Data Controller the school maintains ownership of the data. LexiaUK 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: LexiaUK 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 GDPR compliance.

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

- **ISSUE:** GDPR Training.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to Core5.

- **ISSUE:** Security of Privacy.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: Amazon Web Services hold compliance with ISO/IEC 271001:2013, 27017:2015 and 27018:2019. LexiaUK ICO registration number Z3469808.
  ISO 27001: is one of the most widely recognized, internationally accepted independent security standards.

  ISO 27017: is an international standard of practice for information security controls based on ISO/IEC 27002, specifically for Cloud Services.

  ISO 27018: is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services.

The processing of this data will allow the school to function safely. We know where our students are at any time and can access the vital information we need to keep them safe. We can build up patterns of academic achievement and attitude so that we can best support our students.

Combined staff and student data allows for timetable creation and school organisation with registers.

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 and Workforce). The lawful basis includes the following:

- Childcare Act 2006 (Section 40 (2)(a)
- The Education Reform Act 1988
- Further and Higher Education Act 1992,
- Education Act 1994; 1998; 2002; 2005; 2011
- Health and Safety at Work Act
- 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. The cloud-based solution 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?

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
Data Breaches	Documented in contract and owned by school	Reduced	Low	Yes
Post Brexit	Standard Contractual Clauses in place	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes
Data Retention	Implementing school data retention periods in the cloud	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:	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:

YourIG DPO Service asked the following questions to seek further clarification:

(1) Does Core5 provide the technical capability to ensure the school can comply with rights of access and subject access requests *(i.e. rights to request access, rectification, erasure or to object to processing?)*
What is the cloud-based solution chosen where data processing/storage premises are shared? *(Data is stored within an environment which utilizes state of the art network security, electronic surveillance, physical security and multi factor access control systems along to protect client data?)*

(2) Does the functionality exist to enable the school to apply appropriate data retention periods? *(i.e. the period for which personal data will be stored)*

(3) What certification does Core5 have? *(e.g. ISO 27001 certified, ICO registration)*

The responses have been incorporated in Step 2 of this DPIA under issues, risks and mitigating actions

DPO advice accepted or overruled by:

If overruled, you must explain your reasons

Comments:

DPO Advice Provided

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