STUART BATHURST CATHOLIC HIGH SCHOOL

Data Protection Impact Assessment (Vimeo)

Data Protection Impact Assessment (Vimeo)

Cloud computing is a method for delivering information technology (IT) services in which resources are retrieved from the Internet through web-based tools and applications, as opposed to a direct connection to a server at the school. Stuart Bathurst Catholic High School operates a cloud-based system. 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 moving to a cloud service provider 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 cloud 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 this Data Protection Impact Assessment on an annual basis.

What is the aim of the project?

Stuart Bathurst Catholic High School use Vimeo as a platform for uploading videos in relation to promoting the school and its activities. This can relate to school curriculum, showcasing school facilities, providing a platform for prospectuses, etc.

Many schools use video presentations such as Vimeo embedded and using their website as a platform. Other social media platforms are also used by schools, for example, to widely market good practice within school life. However, having considered these uses, Stuart Bathurst Catholic High School is mindful of the privacy implications.

Where the video features data subjects as defined by UK Data Protection Law and UK GDPR Stuart Bathurst Catholic High School is aware of the privacy implications. Stuart Bathurst Catholic High School is responsible for ensuring that the rights of the data subject are considered and that there is a lawful basis for processing personal data. With this in mind Stuart Bathurst Catholic High School will ensure that any videos uploaded by the school are unlisted, i.e. they do not appear in any search function and the links to the videos in the school's channel can only be shared by the school to the intended recipients (i.e. parents or legal guardians). Additionally, Stuart Bathurst Catholic High School will ensure that there is a lawful basis whereby pupils appear in the video. The lawful basis Stuart Bathurst Catholic High School
is relying on is consent. Vimeo is a video sharing service where users can watch, like, share, comment and upload their own videos. The video service can be accessed on PCs, laptops, tablets and via mobile phones. With this in mind Stuart Bathurst Catholic High School
will undertake the following processes:

1. Collecting personal data
2. Recording and organizing personal data
3. Structuring and storing personal data
4. Copying personal data
5. Retrieving personal data
6. Deleting personal data
7.

By opting for a cloud-based solution the school aims to achieve the following:

1. Scalability
2. Reliability
3. Resilience
4. Delivery at a potentially lower cost
5. Supports mobile access to data securely
6. Update of documents in real time
7. Good working practice, i.e. secure access to sensitive files

Vimeo is a publicly owned independent company listed on the US NASDAQ.

Vimeo enables the school to upload documents, photos, videos, and other files to its website to share with others. Vimeo can then be accessed from any location or any type of device (laptop, mobile phone, tablet, etc.) to the school's website.

Vimeo cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated especially with reference to the storing of pupil and workforce data in the cloud.

Stuart Bathurst Catholic High School will be using Article 6 1 (a) 'the data subject has given consent to the processing of his or her personal data for one or more specific purpose' as its lawful basis for processing personal data.

For the processing of special categories of data Stuart Bathurst Catholic High School will be using Article 9 2 (a) 'the data subject has given explicit consent to the processing of personal data for one or more specified purposes.'

This will also be highlighted in the Privacy Notices (pupil and workforce) for the school.

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

The information collected by the school is retained on the school's website. 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. 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.

Will you be sharing data with anyone?

Stuart Bathurst Catholic High School routinely shares pupil information with relevant staff within the school, schools that the pupil attends after leaving, the Local Authority, the Department for Education, Health Services, Learning Support Services, RM Integris and various third-party Information Society Services applications.

Stuart Bathurst Catholic High School routinely shares workforce information internally with people responsible for HR and recruitment (including payroll), senior staff, with the Local Authority, and the Department for Education.

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. Personal data revealing the racial, ethnic origin, and in some cases health, by taking video recordings will be identified when using Vimeo.

What is the nature of the data?

Where the video features data subjects as defined by UK Data Protection Law and UK GDPR Stuart Bathurst Catholic High School is aware of the privacy implications. Stuart Bathurst Catholic High School is responsible for ensuring that the rights of the data subject are considered and that there is a lawful basis for processing personal data. With this in mind Stuart Bathurst Catholic High School will ensure that any videos uploaded by the school are unlisted, i.e. they do not appear in any search function. Additionally, Stuart Bathurst Catholic High School will ensure that there is a lawful basis whereby pupils appear in the video. The lawful basis Stuart Bathurst Catholic High School is relying on is consent.

Special Category data?

Some of the personal data collected falls under the UK GDPR special category data. Personal data revealing the racial, ethnic origin, and in some cases health, by taking video recordings will be identified when using Vimeo.

How much data is collected and used and how often?

Personal data is collected for pupils and teaching staff appearing in the Vimeo video.

How long will you keep the data for?

The school will be applying appropriate data retention periods as outlined in its Data Retention Policy and the IRMS Information Management Toolkit for Schools.

Scope of data obtained?

Using Vimeo relies on the minimal use of personal data. Data will relate to pupils and staff at Stuart Bathurst Catholic High School

The school provides education to its students with staff delivering the National Curriculum

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?

Access to Vimeo will be controlled by the school.

Cloud Service provider is hosting the data and will not be accessing it.

The school will be able to upload personal data from its PC for the data will be stored on the school's website and remotely by a service provider.

Do they include children or other vulnerable groups?

The personal data will include children. Some of the personal data collected falls under the UK GDPR special category data. Personal data revealing the racial, ethnic origin, and in some cases health, by taking video recordings will be identified when using Vimeo.

Are there prior concerns over this type of processing or security flaws?

Does the cloud provider store the information in an encrypted format? What is the method of file transfer? For example, the most secure way to transfer is to encrypt the data before it leaves the computer. Encryption does have its limitations since the encryption key will need to be shared with others to access the data.

Stuart Bathurst Catholic High School recognises that moving to a cloud-based solution raises a number of General Data Protection Regulations issues as follows:

- **ISSUE:** The cloud-based solution will be storing personal data including sensitive information
  RISK: There is a risk of uncontrolled distribution of information to third parties
  MITIGATING ACTION: Vimeo school data is stored on approved and compliant cloud infrastructure. Access to all parts of the infrastructure is available to Vimeo's staff on a permissions-level basis so that only those members of staff that require access, are granted the appropriate permissions. In addition, Vimeo has 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 Vimeo are encrypted over modern TLS standards. 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 Vimeo 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: Vimeo's servers are hosted by Amazon Web Services located in the United States.

  Access to the servers is restricted to a very small number of employees who require access for systems maintenance and monitoring purposes. Systems are monitored 24/7 and there are full audit trails.

  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 UK/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: Vimeo's servers are hosted by Amazon Web Services in the United States. Vimeo does not have data centres located in other countries

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, ie. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: It is Vimeo's policy to comply with the EEA's General Data Protection Regulation (GDPR). In accordance with the GDPR, Vimeo may transfer personal information from the UK to the United States (or other countries) based upon the following legal bases:

  Legitimate business interests: Vimeo could not provide services or comply with its legal obligations without transferring personal information to the United States.

  Vimeo uses of Standard Contractual Clauses (also known as "Model Clauses") where appropriate in order to meet its obligations of protecting the rights of UK / EU citizens under the GDPR

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Vimeo provides tools in order for a data subject to exercise their rights including opt out of non-essential cookies; access, correct, delete, restrict, or object to use of personal information; be forgotten; port your data; and withdraw consents. Vimeo enables exerting of these rights primarily through their services. For example, allowing users to change their information, download their videos, and close their accounts. Vimeo also fulfils their obligations in response to direct requests which it will endeavor to process requests within one month, where it is able to comply with requests to the extent that they would cause Vimeo to violate any law or infringe any other person's rights. Vimeo will process requests free of charge unless they would impose an unreasonable cost on the company

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: If Vimeo becomes aware of any personal data breach affecting Producer Customer Data, Vimeo will, without undue delay, provide notification to the Producer in accordance with applicable regulations. Vimeo notification of a personal data breach will not be deemed as an acknowledgement by Vimeo of any fault or liability with respect to such incident. In the event of a personal data breach, Producer shall be obligated to take the measures required under applicable laws in connection with its Producer Customer Data. Where requested, Vimeo will assist Producer with communicating with regulators regarding the personal data breach.

  Upon request, Vimeo will make available to Producer information necessary to demonstrate compliance with its obligations under its Data Processing Agreement and applicable law

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Vimeo's servers are located in the United States. Though the company is based outside the UK/EU, Vimeo has stated that it will comply with the UK/EU GDPR through standard contract clauses as defined in its Data Processing Agreement (Schedule 1)

- **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: Data controllers can use the Vimeo Platform administrative consoles and services functionality to help access, rectify, restrict the processing of, or delete any data that they and their users put into Vimeo's systems. This functionality will help the school fulfil its obligations to respond to requests from data subjects when exercising their rights under the GDPR

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school as data controller retains ownership of the data. Vimeo 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: Vimeo through the employment of Amazon Web Services are using its 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.

Amazon Web Services can also automatically scale to meet increased platform demand, by adding or removing capacity as required

- **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.

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

- Scalability
- Reliability
- Resilience
- Delivery at a potentially lower cost
- Supports mobile access to data securely
- Update of documents in real time
- Good working practice, i.e. secure access to sensitive files

The views of senior leadership team and the Board of Governors 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 Legitimate 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
Post Brexit (GDPR noncompliance)	Possible	Significant	Medium
Subject Access Request	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	Data Centre in US, Certified, Penetration Testing and Audit	Reduced	Medium	Yes
Data Breaches	Where applicable documented in contract and owned by school	Reduced	Low	Yes
Post Brexit	Contingency plans 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:	No	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
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		