STUART BATHURST CATHOLIC HIGH SCHOOL

Data Protection Impact Assessment (YouTube)

Data Protection Impact Assessment (YouTube)

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 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 YouTube 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 You Tube embedded and using their website as a platform. Other social media platforms are used 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). 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. YouTube 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

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

YouTube is owned by Google and much of the technological platforms supporting, for example, G Suite for Education and Google Classroom will be similar for YouTube.

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

Google 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 used in YouTube.

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 used in YouTube.

How much data is collected and used and how often?

Personal data is collected for pupils and teaching staff appearing in the YouTube 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 YouTube 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 YouTube 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 to 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 used in YouTube.

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:

YouTube is owned by Google and much of the technological platforms supporting, for example, G Suite for Education and Google Classroom, will be similar for YouTube.

- **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: Google data centers are built with custom-designed servers, running Google's own operating system for security and performance. Google has 700+ security engineers that work around the clock to spot threats early and respond quickly

  Google's data centers use custom hardware running a custom hardened operating system and file system. Each of these systems has been optimized for security and performance. Google controls the entire hardware stack and can quickly respond to threats or weaknesses that may emerge

  Google is the first major cloud provider to enable Perfect Forward Secrecy, which encrypts content as it moves between Google servers and those of other companies.

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred. **MITIGATING ACTION:** Data is encrypted at several levels. Google forces HTTPS (Hypertext Transfer Protocol Secure) for all transmissions between users and encrypts message transmissions with other mail servers and uses Perfect Forward Secrecy (PFS) for all its services. Google also Security (TLS) and utilizes 2048 RSA encryption keys for the validation and key exchange phases. This protects message communications when client users send and receive emails with external parties also using TLS.

  PFS requires that the private keys for a connection are not kept in persistent storage. Anyone who breaks a single key can no longer decrypt months' worth of connections; in fact, not even the server operator is able to retroactively decrypt HTTPS sessions.

- **ISSUE**: Security of data whilst hosted in the cloud
  RISK: Risk of compromise and unlawful access when personal data is at rest
  MITIGATING ACTION: Customer data that is uploaded is encrypted at rest.

  All Google employees are required to sign a confidentiality agreement and complete mandatory confidentiality and privacy trainings, as well as a Code of Conduct training. Google's Code of Conduct specifically addresses responsibilities and expected behaviour with respect to the protection of information

- **ISSUE:** Use of third-party sub processors?
  RISK: Non-compliance with the requirements under UK GDPR
  MITIGATING ACTION: Google Group companies directly conduct most data processing activities required to provide the services. However, Google do engage some third-party processors to assist in supporting these services

  Each data processor goes through a rigorous selection process to ensure it has the required technical expertise and can deliver the appropriate level of security and privacy. Google make information available about Google groupsub processors supporting as well as third-party sub processors involved in those services, and Google include commitments relating to sub processors in current and updated data processing agreements

- **ISSUE:** Understanding the cloud-based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: School data is protected as if it were on its own server. Unauthorized parties cannot access school data. Other customers cannot access school data, and the school cannot access theirs. All user accounts are protected by Google's secure architecture that ensures that one user cannot see another user's data

- **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: Google Cloud Platform (GCP) allows customers to choose to store their data in Europe, North America, or Asia. If applicable the school would specify this location when they configure their application to ensure compliance under UK GDPR

  Google's certification under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks includes the Google Cloud Platform.

  Google have also gained confirmation of compliance from European Data Protection Authorities for its model contract clauses, affirming that Google's current contractual commitments for the Google Cloud Platform fully meet the requirements under GDPR in terms of transfers of personal data from the EU to the rest of the world

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Google provides capabilities and contractual commitments created to meet data protection recommendations provided by the Article 29 Working Party. Google offers to sign EU Model Contract Clauses and a Data Processing Amendment for Google Cloud Platform

  UK GDPR restricts the movement of data from the EU to non-EU countries that do not meet the EU's "adequacy" standard for privacy protection. Processing personal data strictly within the EU is a means of compliance with this regulation

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Google provide tools to make it easy for the school to take its data without penalty or additional cost imposed by Google. Administrators can export customer data in standard formats at any time during the term of any agreement entered into by the school and Google. Google Cloud Platform customers can extract their data using industry standard tools, for which there may be charges.

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Google will promptly inform schools of incidents involving its data in line with the data incident terms in Google's current agreements and the updated terms that apply when the UK GDPR came into force

  Google's security practices are verified and certified by third-party auditors. Google has achieved ISO 27001 certification, which means that an independent auditor has examined the controls present in its data centers, infrastructure, and operation

  Amongst these practices, employees are subject to background investigations based on their level of access. Any employee access is governed by a policy of "least privilege access," which means that access is only granted to the information and resources that are necessary for the execution of the assigned task

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance

MITIGATING ACTION: Google Cloud Platform (GCP) allows customers to choose to store their data in Europe, North America, or Asia. For services based in the United Kingdom data is located at Google LLC in the USA.

UK GDPR data protection law applies to the processing of school information as described in Google's Privacy Policy so the school can exercise its right to request access to, update, remove, and restrict the processing of its information. The school as data controller has the right to object to the processing of its personal data information or export its information to another service

- **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 Google Cloud 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 Google 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. Google 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: Google's application and network architecture is designed for maximum reliability and uptime. Data is distributed across Google's servers and data centers. If a machine—or even an entire data center—fails, school data will still be accessible.

  Google owns and operates data centers around the world to keep the services the school uses running 24 hours a day, 7 days a week

  Google's application and network architecture is designed for maximum reliability and uptime. Google's computing platform assumes ongoing hardware failure, and it uses robust software failover to withstand disruption.

All Google systems are inherently redundant by design, and each subsystem is not dependent on any physical or logical server for ongoing operation. Data is replicated multiple times across Google's clustered active servers so that, in the case of a machine failure, data will still be accessible through another system. Google also replicate data to secondary data centers to ensure protection from data center failures

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Google is subject to independent verification of its security, privacy, and compliance controls. In order to provide this, Google undergo several independent third-party audits on a regular basis

  For each one, an independent auditor examines Google's data centers, infrastructure, and operations

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

  ISO 27017: is an international standard of practice for information security controls based on ISO/IEC 27002, specifically for Cloud Services. Google has been certified compliant with ISO 27017 for Google Cloud Platform

  ISO 27018: is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services. Google has been certified compliant with ISO 27018 for Google Cloud Platform

  The American Institute of Certified Public Accountants (AICPA) SOC 2 (Service Organization Controls) and SOC 3 audit framework defines Trust Principles and criteria for security, availability, processing integrity, and confidentiality. Google has both SOC 2 and SOC 3 reports for Google Cloud Platform

  This means that independent auditors have examined the controls protecting the data in Google's systems (including logical security, privacy, and data center security), and assured that these controls are in place and operating effectively

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 EU, 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: 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		