STUART BATHURST CATHOLIC HIGH SCHOOL

Data Protection Impact Assessment (SchoolCloud)

Data Protection Impact Assessment (SchoolCloud)

Stuart Bathurst Catholic High School operates a cloud-based system or 'hosted solution', called SchoolCloud Parents Evening. Access to SchoolCloud is through the internet. Information is retrieved from SchoolCloud via the Internet, through a web-based application, as opposed to a direct connection to a server at the school. Access to SchoolCloud is through a web browser or mobile phone app. 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?

The school has used paper-based booking systems.

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

SchoolCloud Parents Evening is a hosted system which means that all updates, maintenance and management can be performed in a central location by SchoolCloud Systems Limited.

SchoolCloud is a communications management tool that facilities the booking of meetings between the school and parents. Stuart Bathurst Catholic High School hopes to achieve ease of management of the booking and conducting of meetings by adopting the platform.

The platform provides a number of tools with which to help manage meetings and if necessary, conduct them over a video conference call to support remote discussions.

By employing SchoolCloud, 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 SchoolCloud 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. SchoolCloud 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 SchoolCloud Systems Ltd is the data processor.

Stuart Bathurst Catholic High School has included SchoolCloud 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. SchoolCloud is referenced in the respective Privacy Notices.

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

SchoolCloud collects information from pupil records. Student and staff details are transferred securely from their Management Information System (MIS). The information will be stored in SchoolCloud. 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.

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 SchoolCloud 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. This information is not directly collected by SchoolCloud but may be shared during a live video meeting between the school and parents.

What is the nature of the data?

Pupil data relates to personal identifiers and contacts (such as name, registration class, year group, DOB, MIS ID). Parental contact information that is processed: title, name, relationship to pupil, parental responsibility to student, contact priority, MIS ID and email address.

Workforce data relates to personal information (such as title, name, email address, MIS ID. 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 but is not recorded by SchoolCloud. However, this information may be shared during a video conference call. 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 SchoolCloud Parents Evening. The school can restrict access to SchoolCloud so that only designated staff only see information that is relevant to them. Access to the data held on SchoolCloud will be controlled by username and password.

Additionally, whilst SchoolCloud 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 authorised 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 contact details for meetings, etc.

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

All data is secured in transit using modern SSL 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:** SchoolCloud will be storing personal data
  RISK: There is a risk of unauthorized access to information by third parties
  MITIGATING ACTION: SchoolCloud Systems Ltd school data is stored on approved and compliant cloud infrastructure. Access to all parts of the infrastructure is available to SchoolCloud Systems 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 SchoolCloud installation are encrypted over SSL. The https:// (instead of the normal http://) in the school's browser's address bar denotes a 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 SchoolCloud 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

The schools data is also encrypted at rest in the data centre, only authorised persons are permitted to view the data through the granting of access permissions and UKFast employs a number of safeguards to protect the data within the data centre itself

All staff employed by SchoolCloud Systems Ltd who work on SchoolCloud (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. All persons including those of the hosting company who access to the data are required to pass enhanced disclosure checks

- **ISSUE:** Understanding the cloud-based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: SchoolCloud Systems Ltd's servers are hosted by UKFast, who are located in the United Kingdom. Backups are stored in the EEA by Amazon Web Services (AWS), emails are processed by Help Scout, who are based in the US. Help Scout complies with the EU-US Privacy Shield framework, or Standard Contractual Clauses (SCC's)

  Physical access points to the data centres 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 multiple levels of authentication to access data centers

- **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: SchoolCloud Systems Ltd servers are hosted by UKFast in the United Kingdom to ensure school data is retained within the European Economic Area

- **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 SchoolCloud System Ltd staff can access it. All staff have DBS clearance and have undertaken data protection and information security training

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SchoolCloud Systems Ltd follows the school's data retention policy; data is managed and updated by the school. Personal data is retained for 30 days following the termination of the school's license or after 6 months if using a trial system

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SchoolCloud 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 named SchoolCloud 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: UKFast hold a number of certifications for data protection, including ISO27001 and ISO 9001. Backups are hosted by Amazon Web Services within the EEA. Two months' worth of backups are retained

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SchoolCloud servers are hosted in the UK

- **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: SchoolCloud 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

SchoolCloud Ltd can either provide, or will provide, means for authorised client users to carry out activities directly

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: As Data Controller the school maintains ownership of the data. SchoolCloud 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: SchoolCloud Systems Ltd through the employment of UKFast are using the resilient and secure data centre facilities to host the school's data. This includes not just the physical security aspects such as a 24-hour on-site data centre, but also the supporting infrastructure (both power and connectivity) to remote backup locations

  The school should maintain ownership of the Cloud technologies used ensuring the current and future technologies enable UK GDPR compliance

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

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: UKFast hold compliance with ISO27001:2013, ISO27017:2015, ISO27018:2019, ISO22301:2012 and ISO9001:2015. SchoolCloud Systems Ltd are Cyber Essentials Certified, ICO registration number ZA009035

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

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

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. SchoolCloud 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	Data Centre in UK, Cyber Essentials Certified, ISO 27001	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:	Yes	DPO should advise on compliance, step 6 measures and whether processing can proceed

Summary of DPO advice: Technical recommendations to be clarified with third party as follows:

(1) Does SchoolCloud 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 SchoolCloud have?, *(e.g. ISO 27001 certified, ICO registration)*

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